Benutzerhandbuch

asbLAN*tools*®

Version 2.9.1

Mehr Sicherheit für Windows Netzwerke und Computer

asbLANtools ist eine Software der
asb Systemhaus GmbH

Ausgabe: 2012/03

Alle Rechte an der Software und an der vorliegenden Dokumentation liegen bei asb Systemhaus GmbH. Ein Nachdruck oder Auszug dieser Dokumentation, auch in elektronischer Form, ohne vorherige Zustimmung von asb Systemhaus GmbH, ist nicht zulässig.

Die in der Dokumentation genannten Warenzeichen sind im Besitz der jeweiligen Hersteller.

asb Systemhaus GmbH

Ernst-Kohl Straße 35

99423 Weimar

E-Mail: Info@asb-systemhaus.de

Telefon: +49 (3643) 457 17 10

Fax: +49 (3643) 457 46 09

Aktuelle Informationen finden Sie auf unserem WWW-Server im Internet unter

http://www.asb-systemhaus.de

Hinweis zum Lesen des Handbuches

Es empfiehlt sich, das Handbuch, insofern möglich, über einen Farbdrucker auszugeben.

☛ **Das Kapitel asbLANtools Viewer ist mit farbigen Darstellungen gestaltet, welche die Auswertung von Eigenschaften innerhalb einer Treeview Darstellung mittels farbiger Ikonen, erfordert.**

Bitte beachten Sie auch die Informationen in der Datei README.html im Setup, bzw. auf dem Datenträger. Hier finden Sie die jeweils aktuellsten und letzten Informationen.

Stand
Letzte Korrektur: 2. April 2012
Druckdatum: 2. April 2012

Inhaltsverzeichnis

asbLAN*tools*.....1
Inhaltsverzeichnis 3

1 Einführung..... 7
1.1 Betrachtung zum Konzept 9
1.2 Neue Funktionen in Version 2.9.1 11
1.3 Informationen erfassen (Scannen)..... 13
1.4 Visualisieren und Auswerten 15

2 Übersicht asbLANtools.....18
2.1 Funktionsübersicht..... 18
2.1.1 Systemanforderung..... 18
2.1.2 Modul Administrator..... 19
2.1.3 Modul Viewer..... 19
2.1.4 Lizenzmodell..... 19
2.2 Der Leistungsumfang der asbLANtools..... 20
2.3 Die Arbeitsweise der asbLANtools..... 20
2.4 Arbeiten in großen Netzwerken 22

3 Installation/ Deinstallation/ Update.....24
3.1 Lizenzmodell 24
3.1.1 Demoversion 25
3.1.2 Evaluierungsversion..... 25
3.2 Installationsvorbereitung 26
3.3 Softwareinstallation 27
3.3.1 Profiler Version..... 29
3.4 SQL Server installieren 30
3.4.1 Microsoft SQL Server Varianten..... 30
3.4.2 SQL Express Version..... 30
3.4.3 asbLANtools Datenbank installieren..... 30
3.5 Update / Deinstallation 35
3.6 Datenübernahme/ Datenarchiv..... 36

4 Beschreibung der asbLANtools Module 37
4.1 Voraussetzungen..... 37
4.2 Startmenü..... 38
4.3 Lizenzverwaltung..... 38
4.3.1 Lizenzanforderung..... 38
4.3.2 Lizenzeingabe 39
4.4 Modul Administrator..... 41
4.4.1 asbLANtools Administrator anwenden..... 41
4.4.2 Datenquellen verwalten..... 43
4.4.3 Datenquelle einrichten 44
4.4.4 Administrator-Oberfläche im Detail..... 45
4.4.5 Objekte für ein DatenScan auswählen..... 54
4.4.6 DatenScan Prozess..... 55
4.4.7 Scannen von nicht- Windows konformen Servern..... 56
4.4.8 Protokollierung..... 57
4.5 Modul Viewer..... 58
4.5.1 Übersicht..... 59
4.5.2 Datenbank auswählen..... 60

4.5.3 Bedienoberfläche 61
4.5.4 Informationen suchen 65
4.5.5 Kontext sensitive Menüs 66
4.5.6 Eigenschaftsfenster 67
4.5.7 Analysefunktionen im Detail 69
4.5.8 Auswertung Filesystem /Verzeichnisbäume 75
4.5.9 Filesystem /Berechtigungskonsolidierung 79
4.5.10 QueryManager 81
4.6 Reports 82
4.6.1 Übersicht Reports 86
4.6.2 Arbeiten mit Reports 86
4.7 Modul Batch-Prozessor (asbLTcmd) 88
4.8 Profiler Version 90
4.9 asbAD Active Directory Dump Service 91
4.10 Modul ScanService 95
4.10.1 Dateistrukturen für einen Scan Auftrag 96
4.11 Modul Import Service 97

5 asbLANtools anwenden 100
5.1 Konfigurationshinweise 100
5.1.1 Festlegung eines Domaincontroller (DC) für den Scanprozess 100
5.2 Daten importieren 100
5.3 Automatisierte Datenerfassung 101
5.3.1 Datenbank Import-Service 102
5.3.2 Datenfluss bei Scan- und Import-Service 102
5.3.3 Große Netzwerke 103
5.4 Dezentrale Erfassung 103

6 Tabellen und Übersichten 104
6.1 SQL-Skripts 104
6.2 Report Übersicht 104
6.3 Scan Filedaten 106

7 Fragen und Antworten 107
Abbildungsverzeichnis 109
Tabellenverzeichnis 111
Indexverzeichnis 112

Endbenutzer-Lizenzvertrag für asb Softwareprodukte

Dieser Endbenutzerlizenzvertrag der asb Systemhaus GmbH, nachfolgend „asb" genannt, ist ein rechtsgültiger Vertrag zwischen dem Benutzer der Software („Lizenznehmer") - entweder als natürlicher oder juristischer Person - und asb als Hersteller für das Softwareprodukt.
Durch Installation und / oder Anwendung der Software erklärt der Benutzer seine Zustimmung zu den Lizenzbedingungen der Software. Falls der Benutzer den Bestimmungen dieses Lizenzvertrages nicht zustimmt, ist er nicht berechtigt, das Softwareprodukt zu verwenden und muss dieses unverzüglich deinstallieren/ löschen. Der Lizenznehmer kann es jedoch gegen Rückerstattung des Kaufpreises an den Händler zurückgeben, von dem er es erworben hat. Das Softwareprodukt wird lizenziert, nicht verkauft.

1. Gegenstand des Vertrages
Das Softwareprodukt umfasst Computersoftware sowie möglicherweise dazugehörige Medien, gedruckte Materialien und online- oder elektronische Dokumentationen („Softwareprodukt").

2. Umfang der Benutzung
Der Benutzer der Software ist nur dann berechtigt eine Kopie des Softwareprodukts zu verwenden, wenn diese Nutzung durch a) bezahlten Kaufvertrag vereinbart, oder b) durch einen. im Allgemeinen max. 4 wöchigen kostenfreien Evaluierungszeitraum genutzt wird. Der Benutzer ist verpflichtet die Lizenzbestimmungen für das jeweilige Produkt einzuhalten.

3. Besondere Beschränkungen
Der Benutzer ist nicht berechtigt, das Softwareprodukt abzuändern, zurück zu entwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren. Der Benutzer ist nicht berechtigt, das Softwareprodukt zu vermieten, zu verleasen oder zu verleihen.

4. Evaluierung
Erhält ein Benutzer die Software kostenfrei für einen Anwendertest zur Verfügung gestellt (=Evaluierung), so dürfen gewonnene Erkenntnisse und Daten aus der Evaluierung nur für den Eignungstest der Software selbst verwendet werden. Eine Nutzung der gewonnenen Erkenntnisse und Daten, oder deren Weitergabe mit betriebswirtschaftlichem Vorteil für den Benutzer oder Dritten widersprechen einer Evaluierungsvereinbarung und sind durch einen mindestens einfachen Preis der Lizenzgebühren schadensersatzpflichtig.

5. Übertragung des Benutzerrechtes
Der Benutzer ist berechtigt, alle seine Rechte aus diesem Lizenzvertrag dauerhaft zu übertragen, vorausgesetzt, er behält keine Kopien oder durch die Software gewonnene Ergebnisse in jedweder Form zurück, er überträgt das vollständige Softwareprodukt einschließlich aller Komponenten, der Medien und des gedruckten Materials, aller Updates, dieses Lizenzvertrages und, der Empfänger stimmt den Bedingungen dieses Lizenzvertrages zu. Wenn es sich bei dem Softwareprodukt um ein Update handelt, muss jede Übertragung auch alle früheren Versionen des Softwareproduktes einschließen. Die Übertragung ist asb nachweislich anzuzeigen.

6. Dauer des Vertrages / Kündigung
Der Vertrag beginnt mit dem Erwerb des Produktes und läuft auf unbestimmte Zeit. Das Recht des Benutzers erlischt automatisch ohne Kündigung, wenn er eine Bedingung dieses Vertrages verletzt. In einem solchen Fall ist er verpflichtet, sämtliche Kopien des Softwareproduktes und alle seine Komponenten zu vernichten.

7. Urheberrecht
Eigentum und Urheberrecht an dem Softwareprodukt einschließlich (aber nicht beschränkt auf Bilder, Fotografien, Animationen, Video, Audio, Musik, Text und „Applets", die in dem Softwareprodukt enthalten sind), den gedruckten Begleitmaterialien und jeder Kopie des Softwareprodukts liegen bei asb oder /und Vorlieferanten. Das Softwareprodukt ist durch Urheberrechtsgesetze und internationale Urheberrechtsbestimmungen geschützt. Aus diesem Grund ist der Benutzer verpflichtet, das Softwareprodukt wie jedes andere durch das Urheberrecht geschützte Material zu behandeln, mit der Ausnahme, dass er berechtigt ist, das Softwareprodukt im Rahmen des jeweilig

gültigen Lizenzmodells zu installieren, vorausgesetzt, er bewahrt das Original ausschließlich für Sicherungs- und Archivierungszwecke auf. Der Benutzer ist nicht berechtigt, dass das Softwareprodukt begleitende gedruckte Material zu vervielfältigen.

8. Schadenersatz bei Vertragsverletzung
asb macht darauf aufmerksam, dass der Benutzer für alle Schäden aufgrund von Vertragsverletzungen haftet, die asb aus einer Verletzung dieser Vertragsbestimmungen durch den Benutzer entstehen.

9. Gewährleistung und Haftung
asb garantiert für einen Zeitraum von 6 Monaten ab Empfangsdatum, dass von asb gelieferte Produkte bei normaler Benutzung und Wartung frei von Material- und Verarbeitungsfehlern ist. Die Garantie ist auf 6 Monate beschränkt. Die Garantie von Software ist durch die in der Anwendungsbeschreibung definierten Umgebung eingegrenzt.

Die gesamte Haftung von asb und sein alleiniger Anspruch besteht nach Wahl von asb entweder in der Rückerstattung des bezahlten Preises, in der Reparatur oder dem Ersatz des Softwareproduktes oder der Hardware, die der beschränkten Garantie von asb nicht genügt und zusammen mit einer Kopie Ihrer Rechnung an asb zurückgegeben wird. Diese beschränkte Garantie gilt nicht, wenn der Ausfall des Softwareproduktes oder der Hardware auf einen Unfall, auf Missbrauch oder auf fehlerhafte Anwendung zurückzuführen ist.

asb übernimmt keine Gewähr dafür, dass die Software den Anforderungen und den Zwecken des Lizenznehmers genügt oder mit anderen von ihm ausgewählten Programmen zusammenarbeitet. asb schließt für sich jede weitere Gewährleitung bezüglich der Software, der zugehörigen Handbücher und schriftlichen Materialien und der begleitenden Hardware aus.

Weder asb noch die Lieferanten von asb sind für irgendwelche Schäden (uneingeschränkt eingeschlossen sind Schäden aus entgangenem Gewinn, Betriebsunterbrechung, Verlust von geschäftlichen Informationen oder von Daten oder aus anderem finanziellen Verlust) ersatzpflichtig, die auf Grund der Benutzung dieses asb Produktes oder der Unfähigkeit, dieses Produkt zu verwenden, entstehen, selbst wenn asb von der Möglichkeit eines solchen Schadens unterrichtet worden ist. Auf jeden Fall ist die Haftung von asb auf den Betrag beschränkt, den der Lizenznehmer tatsächlich für das Produkt bezahlt hat. Dieser Ausschluss gilt nicht für Schäden, die durch Vorsatz oder grobe Fahrlässigkeit von asb verursacht wurden. Ebenfalls bleiben Ansprüche, die auf unabdingbaren gesetzlichen Vorschriften zur Produkthaftung beruhen, unberührt.

10. Gerichtsstand
Der Gerichtsstand ist Weimar, Deutschland.

asb Systemhaus GmbH
Ernst-Kohl Straße 35
D-99423 Weimar
Bundesrepublik Deutschland

1 Einführung

In den letzten Jahren hat sich Windows Systeme als Netzwerk-Betriebssystem- und Plattform für Applikationsserver durchgesetzt.
Stabilität, Skalierbarkeit und die Verfügbarkeit in den einzelnen Landessprachen trugen wesentlich zum Erfolg dieses Systems bei.

Für Administratoren ist es relativ einfach, ein kleines Netzwerk in Betrieb zu nehmen. In großen Netzwerken sind die laufende Pflege und Unterhaltung sowie Dokumentationen unabdingbarer Bestandteil. Windows Systeme bieten selbst keine oder nur geringe Möglichkeiten der Dokumentation der einzelnen Systeme und/oder des gesamten Netzwerkes mit relevanten Sicherheitseinstellungen. asbLANtools ist ein Produkt, welches in diese Lücke zielt.

Moderne Windows Systeme arbeiten mit dem Domänenmodell. Benutzerkonten und Gruppen ordnen sich jeweils einer Domäne unter. Durch das Konzept der Vertrauensstellungen und/ oder hierarchischen Domänenstrukturen (Standorte etc.) können Master-Domänen, Ressourcen-Domänen sowie unter Windows Active Directory Strukturen unterschiedlichster Konstellationen Anwendung finden. Dieser hierarchische Ansatz kann gut integriert werden. Unerlässlich ist insbesondere auch für eine Migration von Betriebssystem oder einer Verschmelzung bzw. Trennung von Domänen eine **Dokumentation des Ist-Zustandes**.

Die benötigten Dokumentationen eines Netzwerkes müssen nicht nur die physikalische Sicherheit der Systeme, sondern auch vielmehr die logische Sicherheit dokumentieren. Die Vergabe von Benutzerkonten und die Zuweisung von Benutzerrechten, Privilegien und sonstigen Einstellungen wie Proxys bilden den Schwerpunkt der Dokumentation „der logischen Sicherheit“ eines Netzwerkes. Die Effizienz der Anwendbarkeit, Sicherheit und Stabilität hängt je größer das Netzwerk ist, besondere von einer klaren Zuordnung der „Gegebenheiten“ ab. Diese zu dokumentieren, ist Aufgabe und Zielstellung des Administrators und der Revision des Betreibers. Aufgabe und Zielstellung der asbLAN*tools* ist es, dem Administrator und Revisor die Arbeit zu erleichtern.

In der letzten Zeit hat sich für das Aufgabenfeld Sicherheit, Identifikation, sowie dem Schwerpunkt in der Informationsverarbeitung, dem Zugriffsmanagement neben dem „Identity-Management“ der Begriff Identity-Accessmanagement (IAM) herausgebildet.

Was ist IAM?

Identity-Access-Management. soll klären, „wer welche Zugriffsrechte besitzt und wie diese verwaltet werden. IAM. ist ein Prozess der die Authentifizierung, Zugriffsrechte und die eingeräumten Vorrechte eines digitalen Nutzers verwaltet“. Entsprechend ISO/IEC, JTC umfasst Identity-Access-Management (IAM) 3 Schritte:

- Nutzererkennung,
- Autorisierung und
- Beschaffungsmanagement von Daten.

Die Anliegen der Softwarelösung asbLAN*tools* besteht darin, Mitarbeiter der

Abteilungen Administration und Revision in der Aufgabe der Nachweisführung und Dokumentation dieser 3 Einzelschritte zu unterstützen.- asbLAN*tools* ist ein Produkt für die Lösung von IAM Aufgaben im Windows Netzwerk.

Wie kann der Zugang zu Informationen geregelt werden, so dass jeder nur genau den Zugriff auf die Informationen erhält, den er für die Ausführung seiner Arbeitsaufgaben benötigt?

In der Praxis sind viele IAM Aufgaben nur unvollständig oder ansatzweise realisiert. In den vergangenen Jahren stand in den Firmen (im Zeitalter des Internet-Wachstums) der Schutz des eigenen Unternehmens nach Außen im Vordergrund (Netzwerkzugänge, Virenschutz etc.). Stetig wachsende Netzwerke und veränderte Gefahrenquellen werden jedoch das Augenmerk sehr stark auf IAM Lösungen richten. Entsprechend einer IDC Studie werden 80% aller Schäden (Schadenvolumina) durch Mitarbeiter verursacht und nur 20% durch externe Angriffe. Frost & Sullivan sprich deshalb auch von Zuwachsraten von 20 - 30% p.a. Mit der asbLANtools Softwarelösung soll dem wachsenden Bedarf in diesem Bereich Rechnung getragen werden.

Windows Systeme und das integrierte Active Directory bieten täglich neue und bessere Lösungen zur Beherrschung großer Netzwerke. Trotzdem und vor allem deshalb sind 3-th Party Lösungen zur Gewährleistung einer ausreichenden Sicherheit erforderlich. So ist es zwar immer besser möglich, Netzwerke zu administrieren. Insbesondere mit W2K3 und Active Directory wurden große Fortschritte erreicht, aber die Nachweisfähigkeit, Analyse und Dokumentation (Revision) lassen oftmals noch zu wünschen übrig. So ist es mit MS eigenen Bordmitteln z.B. unmöglich nahezu alle Einstellungen von NTFS Files/ Ordnern darzustellen und auszulesen. Aber genau die „unbekannten" Einstellungen stellen immer ein Sicherheitsrisiko dar.

In der Vergangenheit wurde z.B. mit dem SP6a für Windows NT eine Kompatibilität zu W2K erreicht, aber es existieren eine Menge verdeckter Einstellungen bei NTFS Flags die z.B. nur mit asbLANtools dargestellt werden.

Ebenso wurden im Windows Explorer unter W2K/ W2K3 nur ein kleiner Teil möglicher Einstellungen bzw. Flags angezeigt. Die Folge derartiger „unbekannter" Bits besteht darin, dass Dateien die „angeblich" nicht lesbar sind, gelöscht werden können oder eine „unbekannte" Information enthalten. Dies ist immer mehr oder minder ein Ausgangspunkt Sicherheitsprobleme und Datenverlust.

Ein weiteres Problem und Aufgabenfeld von asbLAN*tools* besteht in dem Vergleich (Soll-Ist/ Differenzvergleich) von administrierten Einstellungen. Die Mächtigkeit und Erfordernis komplexer und wirksamer Werkzeuge birgt auch die Gefahr in sich, dass mit wenigen Handgriffen Rechte und Einstellungen von Hunderten von Benutzern verändert werden können. Sind die „OK-Buttons" für eine administrative Aufgabe erst einmal ausgelöst, hilft dann meistens nur noch eine zeitaufwendige Rückspeicherung von Berechtigungen. Die Verursacher können in solchen Fällen meistens nicht ermittelt werden. Ebenso lassen sich getätigte Einstellungen rückwärts nur schwer ergründen, warum und wann diese eingestellt wurden.

asbLAN*tools* hilft Ihnen einen Teil der täglichen Aufgaben (für den Administrator und

Revisor) zu effektiveren. Der Administrator muss prägnante Daten aus seiner DV Umgebung nicht mehr manuell zusammentragen. Die automatisierten Scanprozesse von asbLAN*tools* nehmen dem Administrator lästige Arbeit ab, dem Revisor ermöglichen Sie jederzeit einen Sicherheitsstand „ohne Admin-Rechte“ offline auszuwerten und für die Betriebswirtschaftler die Kosten durch Minimierung der Gefahrenpunkte (Schadensvolumina) zu senken.

Unternehmen und deren Bilanzen werden in zunehmendem Maß nicht mehr alleine nach Börsen und DAX Werten sondern auch nach der Stabilität der sensiblen „Nervenstränge“ der DV Landschaft bewertet, welche einen immer größeren Anteil eines funktionierenden Unternehmens ausmachen. Die eingesetzte Audit-/ Prüfsoftware wird somit immer wichtiger.

1.1 Betrachtung zum Konzept

Die Prüfung von Berechtigungen erfordert immer den Zugriff auf Objekte und deren Berechtigungen selbst. Im Allgemeinen ist ein umfassendes Abbild aller Berechtigungen eines Systems selbstverständlich nur durch Zugriff „auf höchster Ebene“ = durch „administrative Berechtigungen“ möglich.

Auch asbLAN*tools* benötigt für die Erfassung einzelner Informationen unbedingt administrativen Zugang, sofern die Informationen nicht über Benutzerrechte „lesbar“ sind (was auf der anderen Seite nicht allumfassend der Fall sein kann und darf).

Genau hier liegt einer der Vorteile des Konzeptes der asbLANtools in dem verwendeten Offline-Konzept:
Online-Auswertetools haben den Nachteil, dass Sie während der gesamten Programm-Nutzung einen administrativen Zugriff auf das gesamte Netzwerk erfordern. Dies kann schnell zu unbeabsichtigten nachhaltigen Fehlern führen. Es sollte bei DV Anwendungen der Grundsatz ***„Nur so viele Rechte wie notwendig und nicht so viele wie möglich“*** gelten.
Ferner haben Online-Auswertungs-Systeme den Nachteil, dass sich während der Auswertung/Erfassung in großen Systemen selbst bereits Gegebenheiten ändern können und damit inkonsistente und falsche Aussagen entstehen können.

Im Gegensatz zur „Online“-Auswertung kann asbLAN*tools* die zur Auswertung benötigten Informationen auch in nutzungsschwachen Zeiten (nachts) bereitstellen. asbLAN*tools* bietet Windows-Services für Scan- und Datenbank-Import Aufgaben an. Der ScanService übernimmt „Aufträge“ und speichert die Ergebnisse für eine Auswertung in Ordnern des Filesystems ab.
Diese Ergebnisse können archiviert oder aber, nachdem Sie in eine DB importiert wurden, umfangreich ausgewertet werden.

Weitere Funktionen in Zusammenhang mit ScanService sind:

- Effektiver DatenScan verteilter Informationen in Niederlassungen und Teilnetzwerken (OU)
- Zusammenführung verteilt gescannter Informationen für eine zentrale Auswertung
- Integration von Postprocessing wie Archivierung (Mitteilung, Datensäuberung)

Im Produkt asbLAN*tools* ist die Informationserfassung von der Auswertung getrennt.

Für die Speicherung der Daten werden relationale Datenbanken verwendet. Die offene Datenhaltung ermöglicht die Integration in bestehende Lösungen. Ferner können wahlfreie Werkzeuge bzw. Datenbank-Tools zur Auswertung eingesetzt werden.

asbLAN*tools* unterstützt in der vorliegenden Version die folgenden Datenbanken:

- MS SQL Server der Versionen 2008 / 2008R2

Eine Dokumentation der Datenbankstrukturen finden Sie in diesem Handbuch bzw. gekennzeichneten Anhängen (Aktualisierungen)

Die asbLAN*tools* unterscheiden aus der Sicht der Datenerfassung unterschiedliche Objektklassen:

- Domänen –Information
- Maschine-Information
- Information des Filesystems
- Zusatz-Informationen des Active Directory (Auszug/Filter/Objekt spezifische Auswahl sind möglich)

Diese Informationen sind hierarchisch abhängig im Datenbankmodell verankert, so dass bei einer Auswertung in jedem Fall die übergeordneten Objekte in der Datenbank vorhanden sein müssen.

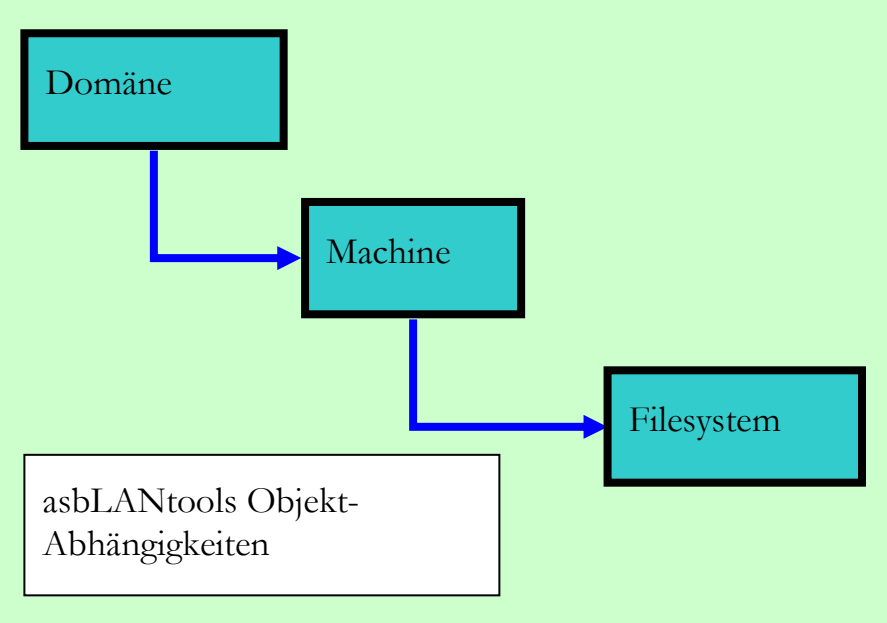


Abbildung 1.1: asbLANtools Objekt-Hierarchie

- Ebene-1: Domänen.
  In Multidomänen Umgebungen sollten alle Domänen, mit denen direkte Vertrauensstellungen bestehen, erfasst werden.
- Ebene-2: Maschinen
  Nur Maschinen, welche Mitglied einer Domäne sind, können erfasst werden. Arbeitsgruppen werden nicht unterstützt.
- Ebene-3: Filesystem
  Filesystem Informationen können über Netzwerkfreigaben erfasst werden. Für NTFS werden alle Zugriffslisten aller Verzeichnisse und Dateien neben den üblichen

Eigenschaften erfasst. Art und Umfang sein einstellbar.
- Zusätzlich zu den im „Domain Scan“ erfassten AD Informationen besteht die Möglichkeit AD Informationen nach eigener Vorgabe /Auswahl zu erfassen.

Zur Sichtbarkeit von Informationen der jeweiligen Objekt-Hierarchie in einer Datenbank ist das Vorhandensein der jeweils darüber befindlichen Ebene erforderlich. Ursache dieser Verfahrensweise liegt in einem „beabsichtigten“ Bruch des relationalen Domänen-Modells, damit z.B. Domänen-Informationen ausgetauscht werden können, ohne die Dateiinformationen zuvor zu löschen.

1.2 Neue Funktionen in Version 2.9.1

Die vorliegende Version wurde umfangreich in allen Teilen der Software überarbeitet. Die bekannte Erscheinungsweise und damit Arbeitsweise bleibt im Wesentlichen erhalten.

Folgende grundlegende Neuerungen sind in dieser Version implementiert:

Neues Datenbankmodell:

Das Datenbankmodell wurde komplett überarbeitet. Neben einer Reduktion des Datenaufkommens wurde Zusatztabellen für „Prozess orientierte“ Datenspeicherung eingeführt.
Eine sehr starke Reduktion der DB als eine Voraussetzung mehr Performance in großen Kundenumgebungen wurde durch die geclusterte Speicherung der Berechtigungs- (ACL) Strukturen erreicht. (TblAcl).
Eine weitere wesentliche Neuerung ist die Einführung von versionsspezifischen Import-Tabellen. Damit können parallel verschiedene, auch alte Scaninhalte in die DB importiert werden. Ferner wurde ein erheblicher Geschwindigkeitszuwachs und Flexibilität neben mehr Datensicherheit in der Prozessverarbeitung erreicht. Die Erfassung / Scan von insbesondere großen Filesystemstrukturen jenseits einiger 100.000 bis einige Millionen Ordnern wartet immer wieder mit „Überraschungen“ auf. Auf Grund der Trennung von Import- und Datenverarbeitung- Auswertungsdaten können diese Probleme zukünftig sauber gesteuert werden.

Prozessorientierte Datenströme:

Sämtliche mit Beginn der Datenerfassung (Scan) entstehenden Daten sind im gesamten asbLANtools Prozess identifizierbar.
Jeder Auftrag „Job“ und darin enthaltenen „Tasks“ können somit verfolgt und identifiziert werden. Ebenso wird ein Datenimport separat durch einen „Identifikator“ markiert, sodass eine Aussage getroffenen werden kann wann die auszuwertenden Daten erfasst, und wann diese in die DB importiert worden.

Neuer Datenimport Prozess:
Der Datenimport Prozess selbst arbeitet in 2 Stufen. Die 1. Stufe (Daten-Loader) ist ein versionsabhängiger Prozess, die 2. Stufe des Datenimports (Daten-Qualifizierung) ein Prozess, welcher die Strukturen für die optimale Auswertung erstellt.
Der gesamte Datenimport Prozess ist so gestaltet, das mehrere Scan, Import und Auswerteprozesse parallel und gleichzeitig laufen können.

Neue Tabellen und Tabellenstrukturen, Datentypen:

Folgende Tabellenstrukturen wurde als optionale Erweiterungen ergänzt:
Streams
Reparse Points
zentrale ACL Verwaltung
Active Directory
Volume Informationen
Device Informationen
Hilfs- und Arbeitstabellen, Indextabellen;

Ferner wurden in der vorliegenden DB Struktur Tabellenspalten auf ein notwendiges Maß gekürzt, was zu einer deutlichen Einsparung von Speicherplatz geführt hat.
Ebenso wurde (teilweise umgesetzt) die Speicherung von Zeitinformationen mit einem LT-spezifischen Zeit-Datentyp mit einer Auflösung im Sekundenbereich eingeführt (SDATE). Dies ermöglicht die Speicherung eines Datumsbereiches von 1922 bis 2068; mit einem Offset „1989-11-09 19:00“ in einem DWORD.
Eine servicefreundliche Umrechnung erfolgt über implementierte SQL Funktionen.
Ebenso wurden Indexwerte in Datentabellen eingeführt, welche zur Verkürzung der Abfragezeiten in Sichten führt.
Alle Datenzugriffe der Auswertungen Reports/Viewer erfolgen über Standard, sowie angepassten komplexe Sichten (wie etwa hierarchische Darstellungen).

Neue Ablage-Strukturen, Ablagen für Scandaten:

Der Vorteil der asbLANtools mit dem bislang genutzten Konzept der Offline Erfassung wurde weiter ausgebaut. Über die bereits oben beschriebene Einführung der „Scan-Task und Job sowie Import“-Prozess Identifikatoren wurde die Datenablage und Datenfile-Struktur neu organisiert .Die wichtigsten Neuerung sind hier:

- Ablage aller Ausgabe /Scandaten in einer LTX Dateistruktur. Diese beinhaltet jetzt alle „Ergebnisse“ eines Jobauftrages.
- Scan LTX Datei ist über Job-Identifikatoren markiert. Der allgemeine Aufbau eines LTX Files sieht wie folg aus:

Default-{T=20111020_135125}-{J=75dbf87fcf974077974485f92e16d3f9}.LTX
<JobName>-<ScanDatum>-<JobID>.LTX

Analog wird zu jedem Prozessschritt (Scan und Import) je ein Logfile .SLOG und .ILOG wie folgt erstellt:

Default-{T=20111011_125506}-{J=75dbf87fcf974077974485f92e16d3f9.SLOG

Default-{T=20111020_144329}-{J=75dbf87fcf974077974485f92e16d3f9}-{IJob=6176e210bd4b4e6ba26b2c49506e27dd}.ILOG

Implementierung einer offenen Datenimport Struktur und LDAP Integration:

Das 2-stufige Datenimportsystem, sowie die Gestaltung offener DB Strukturen ermöglichen eine leichte Integration /Ergänzung bestehender asbLANtools Daten, durch kundenspezifische Anpassungen.

Der Import-Prozess kann nach Ausführung der „Loader" Funktion unterbrochen werden. An dieser Stelle können kundenspezifische Tabellen und Daten integriert werden. Als Beispiel dient hier die AD/LDAP Integration. Je importierter Domain kann ein Auszug aus eine LDAP Scan in eine DB standardmäßig importiert werden. Die Vielzahl der möglichen Auswertungen kann nur ansatzweise implementiert werden. Durch die Integration von z.B. kundenspezifischen SQL Prozeduren und Funktionen können die standardmäßig für Benutzer dargestellten Eigenschaften um eine Vielzahl weiterer AD Eigenschaften, oder gar kundenspezifischer AD Ergänzungen erweitert werden.
(Der asbLTViewer ermöglicht zudem auf zusätzliche Tabellen, Spalten und Abfragen zuzugreifen und diese sowohl als Zusatz.-Eigenschaften, oder in separaten Baumstrukturen darzustellen.

Geänderte, gelöschte Funktionalitäten:

Der aus der Version 2.8 bekannte DifferenceViewer zum Vergleich zweier Datenbankbestände ist in der aktuellen Version nicht mehr enthalten. Er wird zukünftig ab der nächsten Version als integriertes Versionsmanagement verfügbar sein.

1.3 Informationen erfassen (Scannen)

asbLANtools bietet verschiedene Plattformen Informationen zu erfassen(scannen):

- Administrator Oberfläche
- CMD Comandline-Prozessor
- Services (Windows Dienstanwendungen) für Scan- und DB Import.

Dem Modul asbLAN*tools* Administrator wird hierbei die zentrale Rolle zugeordnet.
Nutzen Sie den asbLANtools Administrator für die Einarbeitung in die Software.
Erst wenn Sie die gewünschten Informationen zielsicher auswerten können, beginnen Sie mit der Automatisierung Ihrer Abläufe. Dazu nutzen Sie die Scan- und Importservices, sowie die Comandline-Version für Batch-Automatisierung.
Die Anwendung der Software über CMD Oberfläche beinhaltet eine zusätzliche Option, nachfolgend auch als „Profiler" bezeichnet:
Für Serviceaufgaben /Audits im Revisions-Umfeld/ Einsatz für Systemhäuser, Händler und Dienstleister ist es mitunter erforderlich „in fremden" Umgebungen kurzfristig ohne Installation Daten für eine Analyse zu erfassen.
Dafür steht eine „installationsfreie" Option (auch als Profiler-Version bezeichnet) des Modules asbLTCmd für den mobilen Einsatz zur Verfügung. (Eine Auswertung kann nur über eine installierte Umgebung erfolgen).
Eine Musterdatei für die Anwendung der Profiler-Version liegt als Musterdatei im

Ordner Documentation.

Die Anwendung der Software asbLANtools beginnt (standardmäßig, s.o.) mit der Installation und der Eingabe eines Lizenzschlüssels im Modul Administrator.

Der Aufruf der Software kann sowohl direkt aus dem Programmordner, dem Startmenü, oder über die installierte Ikone asbLANtools auf dem Desktop erfolgen.

Der asbLANtools Administrator wird vorzugsweise nach dem Start mit einer DB Quelle verbunden.

Es besteht aber auch die Möglichkeit als Datenquelle „Offline“ zu verwenden. Die Nutzung von Offline-Ablagen macht Sinn, falls die Auswertung örtlich getrennt vom Ort des Datenscans erfolgen soll (Dienstleister, Außenstellen, Bereitstellung für die Revision, etc.).

Zum Einrichten einer Datenbank schlagen Sie bitte unter „Einrichten Datenbank nach.

Nach dem Start des asbLANtools Administrators und dem Verbinden mit einer Datenbank erhalten Sie in etwa das nachfolgende Bild der Arbeits-Oberfläche des Administrators:

Im Administrator sehen Sie im linken Treeview-Fenster die Darstellung der Domain-Komponenten im Explorer-Stil. Die Objekte wie Domäne, Maschine und Netzwerkfreigabe können für die Erfassung über Menüs ausgewählt oder durch Drag und Drop, bzw. Befehl Auftrag/Hinzufügen eingestellt werden. Hier finden Sie zudem weitere Erfassungsmöglichkeiten (LDAP, Maschinenliste, u.a.).
Mit dem Befehl „Auftrag scannen“ oder Drücken der Start-Ikone werden alle im „Batch“ Fenster eingefügten Aufträge abgearbeitet. Liegt Verbindung zu einer SQL DB vor, werden nach dem Abarbeiten aller Scan-Aufträge die Daten automatisch in eine Datenbank importiert.
Sie können mehrere DB‘s anlegen und gescannte Ergebnisse jederzeit dann importieren, wenn diese benötigt werden sollen.

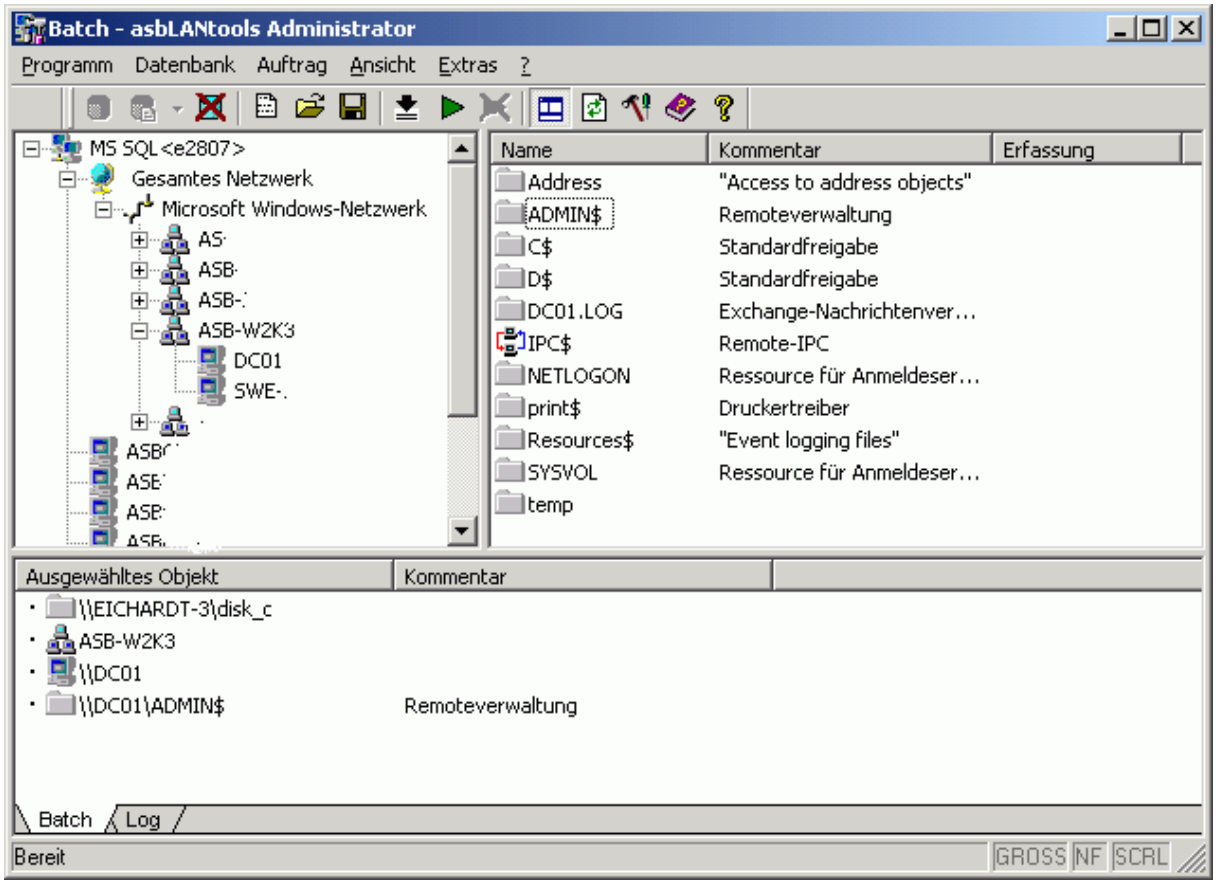


Abbildung 1.2: asbLAN*tools* Administrator Überblick

Zum Auswerten(Anzeigen) und Drucken(Reporting) ist immer eine Datenbank-Verbindung zu einem SQL Server erforderlich.

1.4 Visualisieren und Auswerten

Die hauptsächliche Visualisierung der Informationen erfolgt mit dem Modul asbLAN*tools* Viewer.

Nach dem Starten des Programms asbLTViewer und dem Verbinden mit einer Datenbank wird in etwa die obige Programm-Ansicht mit Ihren Daten sichtbar. Das Bild zeigt eine mögliche Option der Darstellung von Berechtigungen in einem Dateisystem. – Der asbLTViewer ist komplett frei konfigurierbar, sodass Sie die Art und Weise, Umfang und Art der Ansicht eigenständig ändern können. Ebenso können Sie private und sonstige Daten visualisieren.

Das obige „Farbspiel“ der Ikonen kennzeichnet abweichende Berechtigungen einer Datei, eines Ordner, und Abweichungen im Dateibaum. Die Farbe Gelb z.B. kennzeichnet „keine Änderungen“ im Dateibaum.
Zusätzliche Konsolidierungsfunktion zeigen Ihnen z.B. den Vererbungsstatus einer Datei/Ordners und ggf. die „Herkunft der Vererbung“ an.
Die Aufteilung der Programmfensters ermöglicht eine einfache Navigation analog dem asbLAN*tools* Administrator bzw. ähnlich dem MS Windows Explorer. Die unteren Fenster dienen zur Abbildung von Zusatzinformationen.

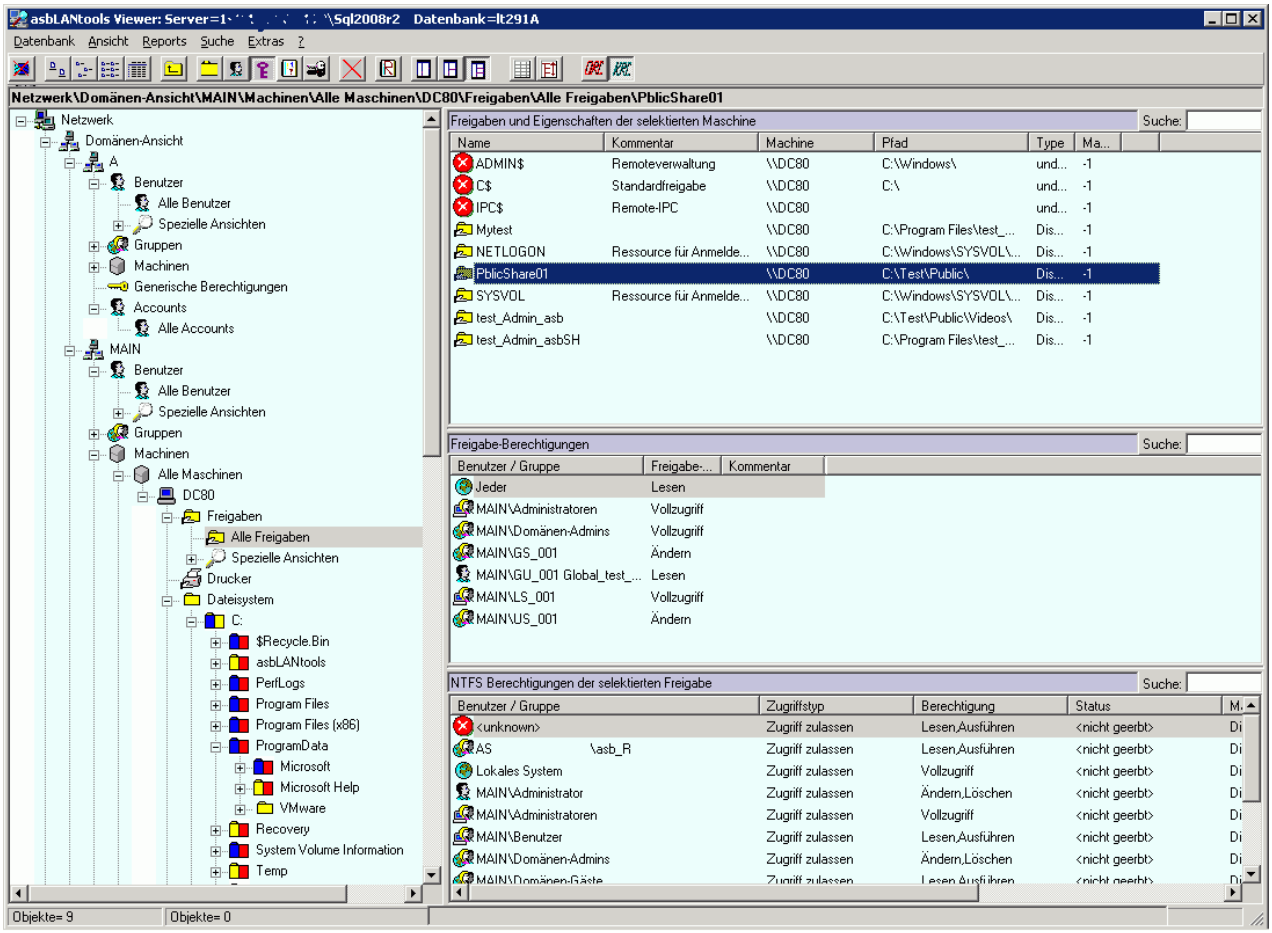


Abbildung 1.3: Einführung asbLAN*tools* Viewer

Über Kontextmenüs (rechte Maustaste) erfolgt die Anzeige/ Auswahl der

- Eigenschaften (Details der Objekte) und
- Reportausgabe (Reports Interface) selektierter Objekte.

Die aktuelle Liste aller bereitgestellten Reports finden Sie im Ordner „Documente“. Reports können über kundeneigene Anpassungen erweitert, selektiert und angepasst werden.

Der asbLANtools Viewer beinhaltet eine Technologie zur dynamischen Registrierung neuer Reports. Sie können somit jederzeit neue Reports zufügen.

Das Konzept von asbLANtools zielt auf eine effektive Auswertung auch komplexer Fragestellungen ab. Hierzu zählen:

- Vertrauensstellungen zwischen Domänen
- SID basierende Aussagen, um auch Aussagen zum „Umbenennen“ von Konten zu ermöglichen und Kollisionen zu vermeiden.
- Änderungen an Objekteigenschaften im NTFS-Verzeichnisbaum werden in der Datenbank gespeichert und im Viewer durch einen farbigen Leitfaden visualisiert.
- Die Bottom-Up Aussagen zu Verzeichnisinhalten und
- Automatische Erfassung aller Rechte(Bitmasken), sowie deren zusätzliche Anzeige in vereinfachten Darstellung (RWDXPO)
- Komplexe Suchfunktionen zum schnellen Auffinden von Dateien

- Reports für ausgewählte Objekte (Multi-Selektion) ist möglich.
- Offenlegung der Datenstrukturen und Schnittstellen für kundenspezifische Erweiterungen.

2 Übersicht asbLANtools

Aus der nachfolgenden Übersicht entnehmen Sie die Einordnung der einzelnen Module bzgl. der Module asbLANtools:

Daten Erfassen (Scan):
- Modul ScanService (Automatisierte Erfassung);
- Modul Administrator (visuelle Unterstützung);
- Modul asbLTCmd (Comandline Version);

Datenbank Import:
- Modul Administrator (visuelle Unterstützung);
- Modul asbLTdbi (automatisierter DB Import);

Administration Voreinstellungen:
- Modul Administrator
- Modul Scan Service Admin
- Modul ImportService Admin

Auswerten von Daten (Visualisieren und Drucken von Reports)
- Modul asbLTViewer; Ausdruck über Crystal Reports.
- kundenspezifische DB Programme
- SQL Server, u.a. Werkzeuge

2.1 Funktionsübersicht

2.1.1 Systemanforderung

- Unterstützte Domänenstrukturen:
  W2k, mixed & native Mode;
  W2k3, alle Modi;
  W2k8 Domänen, alle Modelle;
- Unterstütze SQL Server:
  MS SQL Server 2008, 2008R2 , alle Modifikationen;
- Auswertbare MS Windows Betriebssysteme:
  Windows 2000, XP, 2003/R2, Vista, 2008/R2;
- Plattform für asbLANtools Installation:
  Windows 7 und 2008;
  Windows XP, 2003, Vista, eingeschränkt;
- Unterstützte Datenspeicher-Systeme:
  NetAppliance, CIFS & DAFS konforme Systeme;
- Unterstützte Active-Directory Versionen:
  MS AD-2000, AD-2003 sowie AD-2008 konforme Systeme;
- Administrative Berechtigungen (Domain-Admin) zum Lesen der Daten in der Domäne.
- Windows Domänenstruktur, Workgroups werden nicht unterstützt.

2.1.2 Modul Administrator

- Anzeige der Netzwerkumgebung analog dem Windows Explorer
- Datenerfassung über beliebige(Standard), oder speziell definierbare Domänencontroller (DC) ermöglicht drastische Beeinflussung/ Verkürzung der Erfassungszeiten in WAN Netzwerken.
- Möglichkeit der Beeinflussung der Erfassungszeiten durch optionale Einstellungen, der zu erfassenden Informationen.
- Eingabe /Nutzung von NetBios oder IP Eingaben für Domänen und Maschinennamen

2.1.3 Modul Viewer

- Verwendung von ADO 2.8 Technologie
- Implementierung/ Anwendung von Crystal Reports führt zu leistungsfähigen Reports, welche in verschiedene Formate exportiert, oder gesamt/auszugsweise gedruckt werden können
- Reportumfang ca. 100 anwendbare Reports.
- Komplexe Informationen werden durch prozedurale Unterstützung aufgearbeitet und lesbar dargestellt, Beispiel (Vererbung von Daten, Abweichungen von Berechtigungen im Dateisystem)

2.1.4 Lizenzmodell

- Lizenzierung erfolgt nach Anzahl der Accounts in der/den zu erfassenden Domäne(n), oder einer Teilstruktur; Es können mehrere unterschiedliche Domänen-Teilstrukturen für eine Lizensierung gleichzeitig benutzt werden (Beispiel User und Maschinen in getrennten OU's).
- Die Account-Zählung erfolgt analog dem MS NTLM Standards (Maschinen-und Benutzer-Accounts).
- Multi-Domain Unterstützung:
  Es können gleichzeitig mehrere Domains oder Teildomains lizenziert werden;
- Ferner ist die gleichzeitige Verwendung mehrerer Lizenzen mögliche (Dienstleister).
- Eine Lizenz wird anhand der Domänen SID bzw. Domäne Namen erstellt. Sie umfasst die Programme der Datenerfassung und Datenauswertung.
- Evaluierungslizenz:
  Evaluierungslizenzen besitzen eine zeitliche Eingrenzung der Programmnutzung.
- Einschränkungen in der Evaluierungslizenz:
- Nicht für den produktiven Betrieb erlaubt.
- Erfasste Daten werden nur teilweise ca. 40..50% in Klarschrift dargestellt.
- Drucken auf eine Seite je Report begrenzt.
- Kein Einsatz der Scan und Importservices.
- Kein Einsatz des LDAP-Scanners.
- Für die aktuelle Version wird für alle Module eine gültige Lizenz notwendig. (diese betrifft auch die Module LTViewer und asbAD LDAP Scanner.

- Priorisierte Accounts (vordefinierte Auswahl, max. 10 Accounts)
-

2.2 Der Leistungsumfang der asbLANtools

Microsoft Windows wurde in den letzten Jahren zur führenden Plattform in PC-Netzwerken. Die gestiegenen Anforderungen der Sicherheit und des Datenschutzes verlangen umfassende Dokumentationen der Netzwerke und der Rechte der Benutzer.

Die asbLAN*tools* sind ein Reporting- und Dokumentationswerkzeug für Administratoren und Revisoren.

Die Kernkompetenz der Kernpunkt der asbLAN*tools* bestehen in der Verwaltung und Analyse von Konten und Rechten von Windows Domänen.

Die asbLANtools ermitteln

- Konten und Gruppen von Windows Domänen
- Computer, die Mitglied einer Domäne sind
- Freigaben, Dienste und Konten je Maschine (nur Windows)
- Benutzerrechte je Maschine und Domäne
- Informationen zu Dateien und Verzeichnissen
- Zugriffsrechte im NTFS Dateisystem.

asbLANtools ist nur in Domänenumgebungen einsatzfähig. Arbeitsgruppensysteme werden nicht unterstützt.

Sie können innerhalb einer Domäne Informationen von

- Domänencontrollern
- allein stehenden Servern innerhalb einer Domäne
- Windows Arbeitsstationen

erfassen. Die ermittelten Informationen müssen für eine Auswertung in einer Datenbank gespeichert werden. Bei verteilten Netzwerken (WAN) können die Ergebnisse eines Datenscans (Erfassung) auch in einem als „Offline-Datenquelle“ im Administrator gekennzeichneten beliebigen Verzeichnis gespeichert werden.

Für die Auswertung stehen Berichte zu Verfügung, welche sowohl auf die Gesamtheit der jeweiligen Datenmenge oder nur auf eine spezifische Auswahl angewendet werden können. Eine Übersicht der verfügbaren Reports finden Sie im Dokument „Reportübersicht.PDF“ im Verzeichnis „Documents“ der Programm Installation.

2.3 Die Arbeitsweise der asbLANtools

Die asbLAN*tools* wurde für die Offline Erfassung und Auswertung entwickelt. Der Vorteil besteht darin, dass keine Wartezeiten notwendig sind und am Bildschirm auf die Übertragung der teils recht umfangreichen Informationen gewartet werden muss.

asbLANtools Konzept verfolgt nicht den Ansatz der Administrations-Unterstützung von Netzwerken sondern vielmehr den Ansatz der „Analyse und Auswertung von „Sicherheits-Einstellungen“, sowie die Analyse für vorbereitende und Hilfs-Prozesse des Administrators. Das Hauptanwendungsgebiet der asbLANtools sind Aufgabenstellung der EDV Revision.
Insofern kann asbLANtools auch für die „gute Arbeitsweise“ eines Administrators ein wertvolles Hilfsmittel darstellen. Beispiele dafür sind komplexe Reports welche Aussagen über

- Nicht verwendete Benutzer oder Gruppen
- Verletzung von Einstellungen
- Nutzung /Nichtnutzung von Accounts Gruppen im System etc.

usw., liefern.
Stetig wachsende Komplexitäten verlangen zur Minimierung der Administrationsaufwendungen vor allem Übersicht. Das bietet asbLANtools in vielfältiger Form. Denn gute Übersicht ist der beste Schutz gegen Gefahren.

Zudem kann asbLANtools im Rahmen der Lizenz an verteilten Standorten installiert werden und die Information in einer Datenbank zur Auswertung zusammen geführt werden.

Folgende Komponenten finden dabei Anwendung:

- Scannen der Daten
  mit dem asbLAN*tools* Administrator (siehe Kapitel 4.4), ScanService oder dem Batch-Prozessor (siehe Kapitel 4.11) werden die Informationen im Netzwerk ermittelt und in der Datenbank gespeichert.
- Visualisierung der Daten
  über Modul Viewer (siehe Kapitel Viewer 4.5). Die im LTViewer integrierten Berichte ermöglichen einen formatierten Ausdruck. Der asbLAN*tools* Viewer visualisiert die Informationen in einer durch Windows NT bekannten Form. Für alle Objekte stehen Eigenschaftsdialoge zur Verfügung, mit denen die erfassten Informationen angezeigt werden.
- Reporting über Modul Viewer. Zusätzlich benötigte Reports können leicht eingefügt werden. Die Dokumentation der notwendigen Voraussetzungen finden Sie im technischen Handbuch und den Anlagen.

2.4 Arbeiten in großen Netzwerken

asbLANtools ist geeignet für den Betrieb in großen Netzwerken /Domänen. Sowohl Funktionen als auch das Modulkonzept sind geeignet, dezentral eingesetzt zu werden. Ebenso sind struktur- und programminterne Datenfelder entsprechend ausgelegt. In Verbindung mit dem dezentralen Einsatz mehrerer Datenbanken können individuell zugeschnittene Auswertungen erstellt werden. Das Reporting-System ermöglicht mächtige und komplexe SQL basierende Auswertungen.

Die Erfassung von großen Datenbeständen kann sowohl über den Modul „asbLTCmd", als auch noch optimaler über den „ScanService" und ImportService Modul automatisiert werden.

Für gemischte Netzwerkumgebungen besteht die Möglichkeit alle Datenquellen über IP- und /oder den vollständigen DNS Namen anzusprechen. Generell erfolgt intern immer eine IP Auflösung. Ebenso kann für die Eingabe einer Domäne der jeweils zu nutzende Domänencontroller oder DNS Name angegeben werden. Dies ist dann insbesondere von Bedeutung, wenn Auflösungsprobleme des DNS / Domäne vorliegen könnten.

Für den Scan großer Datenbestände(Domäne/Maschine/Filesystem) ist im Allgemeinen die Erfassung des Filesystems der aufwendigste Prozess. Hier gilt es vorab festzulegen, welche Scan-Optionen anzuwenden sind: Verzeichnistiefe, Erfassung von File (mit Eigenschaft FileSecurity, Streams, Reparse-Points, u.a.). Die Erfassungszeit kann so um Faktoren 1 bis 50 beeinflusst werden .Die Erfassung einer Datei ist ebenso aufwendig wie die eines Directorys. Rein statistisch befinden sich 30 Files in einem Directory, woraus alleine ein Faktor 30 in der Scanzeit resultiert. Ferner wird die Erfassung durch „ein vollständiges" Logfile ausgebremst.

Die besten (effektivsten) Scanzeiten werden zudem beim Einsatz des Scan-Services asbLTS erreicht.

Domänenstrukturen (Benutzer & Gruppen etc.) können als Faustregel ca. 100.000 Accounts in 2 Stunden erfasst werden. Die benötigte Zeit ist dabei abhängig vom Netzwerk, Belastung, Antwortzeiten u.a. Für die Erfassung von Dateisystemen kann keine Faustregel angegeben werden, da die Erfassungszeiten sehr stark schwanken und vom Zustand des Netzwerkes abhängig sind. (Hier treten Schwankungsbreiten bis Faktor 20 in der Praxis auf. Es sind immer individuelle Erfahrungen zu sammeln.)
In jedem Fall ist für den Einsatz der asbLANtools in größeren Netzwerken ein minimales Konzept zu erstellen und die Frage der Notwendigkeit zu beantworten, welche Daten zu erfassen (scannen sind). Die Minimierung des DatenScan von „nur" Ordnern anstatt „Files + Ordner" reduziert in der Praxis die Erfassungszeit auf beispielsweise ca. 3%.
Ebenso ist die Festlegung, ob Systeme „lokal" oder „remote" erfasst werden, von zentraler Bedeutung. Ggf. muss /Kann die Software mehrfach installiert werden um

einen effektiven Scan zu erreichen.

Von einer Erfassung über WAN Leitungen mit schlechten Latenzzeiten raten wir dringend ab.

Müssen Sie als Dienstleister dezentrale Domains, Server oder Filesysteme erfassen, setzen Sie entweder eine „lokale“ Installation asbLANtools ein, oder wenden die Erfassung von Daten über „Profiler“ Option des Modules asbLTcmd an.

3 Installation/ Deinstallation/ Update

Voraussetzungen:

- Für Plattform asbLANtools, bzw.LT Module:
  Windows 07 oder Windows W2k8, R2 , Domänenstruktur (ab W2k Domain)
  Service Pack 1
- Auswertbare Systeme /Betriebssysteme:
  W2k, XP, W2k3, Vista, Win07, W2k8, W2k8R2
- Active Directory
- Server /Workstation mit W2k8/ W7, W2k3, Betriebssystem
  * aktuelles Servicepack.
  Version 2.9.1 ist nicht mehr für Windows XP geeignet, kann jedoch für Windows XP speziell aktiviert werden.
- Lesen Sie zu aktuellen Details auch die README Datei im Installationsverzeichnis.
- Mind. 4 GB Hauptspeicher. virtuell,
- Mind. 300 MB freier Plattenplatz für Software-Installation
- Ausreichend Plattenplatz für die Datenbank.
  Als Richtwert gelten 1% des Gesamtvolumens der zu erfassenden Informationen für die Datenbank.
- Administrative Berechtigungen zum Lesen der Daten in einer Domäne (Domain-Admin)

Datenbank :

- MS SQL Server 2008 / 2008 R2 in verschiedenen Ausprägungen
  (MSDE, Standard, … Enterprise Version je nach Anforderung)

asbLANtools Software .

- Lizenzkey (für Evaluierungs- oder Vollversion).

3.1 Lizenzmodell

Die Lizenzierung der asbLANtools erfolgt pro Domäne und Anzahl der Accounts je Domäne (Benutzer und Maschinenkonten).

Die erforderliche Lizenzgröße können Sie am einfachsten im Startmenü asbLANtools unter der Schaltfläche „Lizenzermittlung“ einsehen.

Lizenzen werden in Schritten von je 100 Accounts ausgestellt.
Als Account werden alle in der jeweiligen Domäne angelegten Accounts entsprechend NTLM Modell in Windows Umgebungen gewertet.

Eine Lizenz zum Scan bzw. Erfassen von Informationen innerhalb einer oder mehrere

Domänen ist abhängig von:

- Domänenname
- Zahl der NTLM Accounts (Objekte) = Summe der Domänen Accounts

asbLAN*tools* kann gleichzeitig mit mehreren Domänen arbeiten, bzw. auch Informationen vertrauter Domänen, oder mehrerer einzelner Domänen auswerten. Ebenso ist eine Lizenzierung einer Standort- bzw. Substruktur möglich.

Je Domäne ist eine Lizenz separat erforderlich.

Für Großkunden werden Firmenlizenzen ausgestellt. Die Formen der Lizenzierung tragen vielfältigen Anforderungen der asbLAN*tools* Kunden Rechnung (Zeitbegrenzte Lizenz, Evaluierung, usw.

Generell werden für die Software bereitgestellt:

- Demoversion
- Evaluierungsversion
- Vollversion, Domänen gebunden
- Händlerlizenz.

3.1.1 Demoversion

Für einen ersten Einblick in die Software asbLANtools werden Demodaten bereitgestellt. Diese beinhalten „gescannte“ Daten in einer oder mehreren vorbereiteten Datenbank.
Die Demo-Datenbank ermöglicht einen Einblick in die Leistungsfähigkeit der Software, Umfang der Daten und Möglichkeiten der Auswertung. Die Demoversion bietet so beste Möglichkeiten zu entscheiden, ob asbLANtools Software die gewünschten Informationen für Ihre geforderten Aufgabenstellungen liefert. Sie können an Hand der Demoversion beurteilen ob die Software für Sie geeignet ist.
Die zusätzlichen Anforderungen an die Datenerfassung (Scan) können durch die Evaluierungsversion abgedeckt werden.

3.1.2 Evaluierungsversion

Die Evaluierungsversion bietet Ihnen einen Einblick in die Software mit Ihren Daten im Netzwerk. Die Evaluierungsversion dient dazu, den komplexen Prozess der Datenerfassung im Netzwerk zu testen und die Möglichkeiten der Auswertung zu beurteilen.

Sie erhalten eine Aussage über Scan Zeiten Ihrer realen Serverdaten sowie eine Aussage über die Machbarkeit des DatenScan.

Mit dem Modul Viewer können Sie testweise Daten auswerten.

Die Evaluierungsversion rechtfertigt nicht zur Verwendung der Ergebnisse aus den asbLANtools für betriebliche Aufgabenstellungen. Bitte beachten Sie dazu auch die Lizenzbestimmungen, Absatz 4).

- Einschränkungen in der Evaluierungslizenz:
- Nicht für den produktiven Betrieb erlaubt.
- Erfasste Daten werden nur teilweise ca. 40..50% in Klarschrift dargestellt.
- Drucken auf eine Seite je Report begrenzt.
- Kein Einsatz der Scan und Importservices.
- Kein Einsatz des LDAP Scanners.
- Priorisierte Accounts (zusätzliche vordefinierte Auswahl, max. 10 Accounts)

3.2 Installationsvorbereitung

Die Software wird über

- CD-ROM /DVD oder
- Download /Internet

bereitgestellt.

Das Installationskit, sowie die Vollständigkeit der Daten kann über FICSV Prüfcode auf Fehler getestet werden. Der im Installationkit enthaltene Prüfcode wird ferner auf der Webseite unter WWW.asb-systemhaus.de veröffentlicht. Damit können Änderungen am Installationskit zur Sicherheit überprüft werden.

Für die Installation benötigen Sie administrative Berechtigungen sowie entsprechende Voraussetzungen, siehe auch Punkt 3).

Den aktuelle Version eines kostenfreien MS SQL Servers der Version SQL2008 /R2 finden Sie auf der Webseite von Microsoft. Bitte beachten Sie, dass der Einsatz eines kostenfreien SQL Servers (Express Edition) speicherplatzbegrenzt ist (2/4 GB).

Eine MS SQL Server Lizenz ist nicht Bestandteil des Produktes asbLANtools, diese müssen Sie separat erwerben.

3.3 Softwareinstallation

Für die Installation und Anwendung der Software benötigen Sie einen geeigneten Rechner. Die Eignung hängt von der Aufgabenstellung und Größe der Domäne /Netzwerkes, maßgeblich der veranlagten Filesysteme ab. Ferner ist ein leistungsfähiger SQL Server erforderlich.

Richtlinien über die Eignung Ihre Hardware-Plattform können nur ansatzweise gegeben werden. Wir beraten Sie dazu jedoch gern. In jedem Fall sind eigene Erfahrungswerte zu sammeln. Für größere Projekte ist ein separates Einsatzprojekt anzuraten.

Die Installation der Software asbLANtools besteht aus 2 Teilen:

- Installation der Softwareumgebung
  Hierzu führen Sie die Installationsscrips auf dem Datenträger /Download Datei aus. Sie erhalten generell 2 Installationsfiles:
  - asbLANtolls_291.xy (xy = aktuelle Release)
  - asbLAntools_291_Environment
  Führen Sie zuerst die Environment Installation aus. Diese prüft Ihre 32/64 Bit Umgebung und installiert ggf. erforderliche Systemdetails.

  Nachdem sie die Umgebung „eingestellt" haben, führen Sie das eigentliche Software Setup aus. Folgen Sie den Installationsdialogen.
  Im Anschluss, oder auch später sollten Sie ggf. die Orte für die Datenspeicherung anpassen.
  Für die SW Installation benötigen Sie administrative Berechtigungen.

- Installation der Datenbank

Für die Auswertung von Daten benötigen Sie eine, oder mehrere installierte SQL Server DBs. Sie können beliebig viele Datenquellen einrichten.

Je nach Art der Installation müssen Sie eine „Mustervorlage" für die Erfassung Ihrer eigenen, erfassten Daten (Über einen DatenScan), oder eine Demo-Datenbank mit gefüllten Daten für eine ausschließlich, musterhafte Auswertung in einem SQL Server „montieren". Dieser Prozess wird im Kapitel „Datenbank einrichten" näher erläutert.

Voll- Demo-und Evaluierungsversion unterscheiden sich nur im Lizenzkey. Insofern steht nur eine Installation zur Verfügung.

Zur Installation benötigen Sie administrative Berechtigungen. Führen Sie das Setup Programm aus und folgenden der Dialog geführten Installation.
Nach Abschluss der Installation stehen Ihnen alle Module lokal auf dem installierten Rechner zur Verfügung. Sie können die Installation innerhalb der „Lizenz-Grenzen" beliebig oft installieren.

Melden Sie sich zur Installation der Software als Domänen-Administrator

(Hauptbenutzer etc. Benutzer mit ausreichend Berechtigungen in Ihrer Umgebung) an, damit Sie die Software installieren können. Halten Sie die notwendige Lizenzdatei bereit.

Über Internet-Download bzw. Programmverzeichnisse können die Installationsdaten zusätzlich gepackt sein.

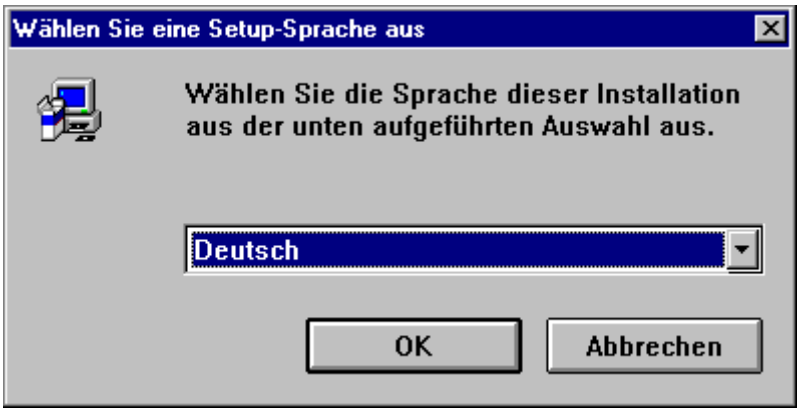

Wählen Sie eine Setup-Sprache aus
Wählen Sie die Sprache dieser Installation aus der unten aufgeführten Auswahl aus.
Deutsch
OK
Abbrechen

Abbildung 3.1: Setup Sprachauswahl

Wählen Sie mit dem ersten Dialog die Sprachversion zu asbLANtools aus. Die Programme selbst sind multilingual ausgelegt. Die Installation wird dann in der gewählten Sprache fortgesetzt.- Derzeit steht für 2.9.1 Release nur die deutsche Ausgabe bereit:

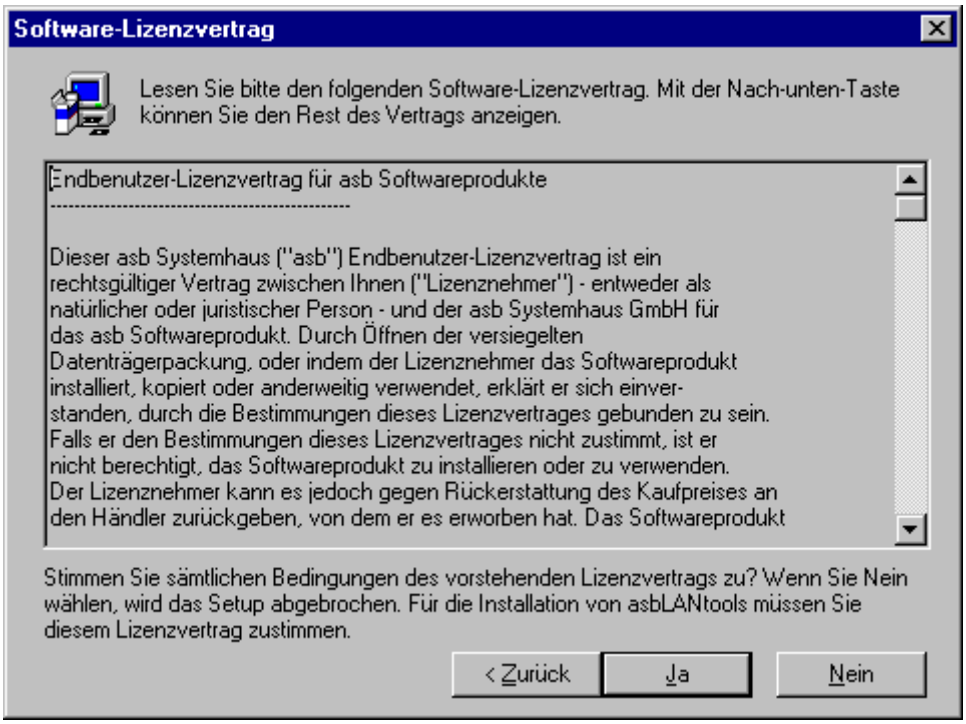

Software-Lizenzvertrag
Lesen Sie bitte den folgenden Software-Lizenzvertrag. Mit der Nach-unten-Taste können Sie den Rest des Vertrags anzeigen.
Endbenutzer-Lizenzvertrag für asb Softwareprodukte
Dieser asb Systemhaus ("asb") Endbenutzer-Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen ("Lizenznehmer") - entweder als natürlicher oder juristischer Person - und der asb Systemhaus GmbH für das asb Softwareprodukt. Durch Öffnen der versiegelten Datenträgerpackung, oder indem der Lizenznehmer das Softwareprodukt installiert, kopiert oder anderweitig verwendet, erklärt er sich einverstanden, durch die Bestimmungen dieses Lizenzvertrages gebunden zu sein. Falls er den Bestimmungen dieses Lizenzvertrages nicht zustimmt, ist er nicht berechtigt, das Softwareprodukt zu installieren oder zu verwenden. Der Lizenznehmer kann es jedoch gegen Rückerstattung des Kaufpreises an den Händler zurückgeben, von dem er es erworben hat. Das Softwareprodukt
Stimmen Sie sämtlichen Bedingungen des vorstehenden Lizenzvertrags zu? Wenn Sie Nein wählen, wird das Setup abgebrochen. Für die Installation von asbLANtools müssen Sie diesem Lizenzvertrag zustimmen.
< Zurück
Ja
Nein

Abbildung 3.2: Setup Lizenzbedingungen

Die Installation der Software erfordert die Anerkennung der Lizenzbestimmungen zum Einsatz des Produktes asbLANtools

Falls Sie den Lizenzbestimmungen nicht zustimmen, müssen Sie die Installation abbrechen. Folgen Sie im Weiteren den Installationsdialogen.

Für die Auswahl des Zielverzeichnisses können Sie jedes beliebige Verzeichnis auf einem Laufwerk festlegen. Ca. 100 MB Programmdateien werden im Systembereich

erforderlich.

Die standardmäßig festgelegten Arbeitsverzeichnisse (siehe Modul Administrator) können manuell nach Installation auf andere Verzeichnisse zugewiesen werden.

Mit Installation(Environment Setup) werden alle erforderlichen Einrichtungsdaten für

- MS SQL2008 / R2

installiert

Nach Abschluss der Installation erfolgt der Aufruf der Liesmich.Html (Readme.Html) Informationsdatei. Lesen Sie diese Datei, sie enthält die letzten aktuellen Informationen. In einigen Fällen kann das Setup von asbLAN*tools* einen Neustart des Rechners erzwingen. Dies tritt auf, wenn Systemkomponenten aktualisiert werden müssen. Führen Sie den Neustart nach Aufforderung durch. Damit ist die Installation der asbLAN*tools* Software abgeschlossen.

Im nächsten Schritt müssen Sie manuell die erforderlichen Datenbanken einrichten. (Siehe Abschnitt Einrichten einer Datenbank)

3.3.1 Profiler Version

Die Profiler Version von asbLANtools stellt eine spezielle, Registry-freie Installation dar, sie dient dem mobilen Einsatz von asbLANtools für Händler und Systemhäuser und unterstützt nur „Erfassungsprozesse“.

Im Gegensatz zu einer „Standard-System-Installation“ über Setup.exe werden in der Profiler Version alle Einstellungen in einem speziellen Profil gespeichert und verwaltet.

Die Anwendung der Profiler-Version ist auf die Nutzung der Funktion „DatenScan“ über asbLTcmd beschränkt.
Auswertungen über LTViewer, Erfassung über Dienste und Nutzung des Administrators, etc. setzt eine Standardinstallation voraus.

Die Profiler Version können Sie über eine vorbereitetes Medium (USB Stick) oder anderen Datenträger in einem fremden Netzwerk aktivieren (ggf. kopieren Sie die Programmmodule (aus Ordner Images) und richten die Daten-Ordner manuell, entsprechend Profile Einstellungen ein.

3.4 SQL Server installieren

asbLANtools erfordert den Einsatz eines Microsoft SQL Servers.
Für alle Datenbanken benötigen Sie ausreichenden Festplattenplatz.
Als Richtwert für Datenbanken gelten:

ca. 1% des Datenvolumens der zu erfassenden Domäne /Speicherplatz.
Die genau Datenmenge ist von verschiedenen Werten abhängig:
Zu erfassende Filesysteme;

- Anzahl Berechtigungen je Objekt;
- Maßgeblich von Einstellung File Scan, Verzeichnistiefe „..
- weitere Optionen

Die Größe der erfassten Datenmenge kann drastisch durch eine Minimierung der gescannten Detail-Information (z.B. der File-Informationen) reduziert werden.
Eine Entscheidung keine Files zu erfassen reduziert das Datenaufkommen um Faktor 20..30; Sie sollten immer mit möglichst geringen Datenaufkommen beginnen.

3.4.1 Microsoft SQL Server Varianten

Folgende MS SQL Server können in der aktuellen Version verwendet werden:

- MS SQL Server 2008
- MS SQL Server 2008R2, 32 oder 64 Bit Version.

3.4.2 SQL Express Version

Als kostengünstige/kostenfreie Variante eines MS SQL Servers kann für kleinere Umgebungen bzw. zum Test eine Runtime /Express Version eingesetzt werden.

Das speicherbare Datenvolumen der verfügbaren Express 2008 Version ist auf 4,0 GB begrenzt. Die Grenzen anderer Runtime Versionen können sich unterscheiden, informieren Sie sich hierzu bei Microsoft.

Sofern möglich setzen Sie eine MS SQL Vollversion entsprechend des MS Lizenzmodells ein.

3.4.3 asbLANtools Datenbank installieren

Sie können beliebig viele Datenbanken für asbLANtools anlegen.

Zum Erstellen einer Datenbank verwenden Sie die Kopie der mit Installation im Programmbereich unter „Program Files\asb Systemhaus\asbLANtools291\Databases“ Muster_LT291.MDF oder eine mit Demodaten gespeicherte DB.

Generell benötigen Sie für das Anlegen einer Datenbank SQL Kenntnisse und Berechtigungen des DB Administrators.

Es gibt mehrere Möglichkeiten des Anlegens einer neuen Datenbank.

- Einbinden einer Kopie einer Mustervorlage über SQL Manager.
- Einbinden einer Kopie einer Mustervorlage über SQL Befehl.

- Einbinden einer Kopie einer Mustervorlage oder Demo-DB über Modul LTViewer.

Anlegen einer neuen DB aus einer Mustervorlage

Die Einrichtung einer neuen Datenbank wird wie folgt ausgeführt:

- Wählen Sie einen geeigneten SQL Server für die Arbeit mit asbLANtools aus. Für die Abschätzung der Anforderungen an einen SQL Server sind einige Daten und Erfahrungen erforderlich. Sie erhalten hierzu gern Unterstützung durch asb Systemhaus.
- Voraussetzung zur asbLANtools Nutzung ist die vorhandene Installation (Instanz) eines MS SQL Servers der Version 2008/R2. Sie können dazu jeden im Netzwerk erreichbaren Server erforderlicher Leistungsklasse nutzen. Die Anforderung hängt im Allgemeinen von der Größe der Netzwerkumgebung, welche mit asbLANtools verwaltet werden soll, ab.
  Die MS SQL Installation ist nicht Gegenstand und Betrachtung der asbLANtools.
  Mit asbLANtools werden auch keinerlei MS SQL Server Bestandteile oder Teile ausgeliefert.
  Bitte sichern Sie im Unternehmen die Bereitstellung eines MS SQL Servers und der erforderlichen Lizenzen ab. Ggf. können Sie (zum Test oder für kleinere Unternehmen durchaus geeignet) auf so genannte Runtime-Lizenzen kostenfrei zugreifen.
- Installieren Sie einen MS SQL Server 2008 Express/Runtime Version auf dem DB-Server/ Arbeitsrechner (insofern Sie keine vorhandene SQL Installation nutzen können. Nähere Informationen siehe dazu bei Microsoft.
- Die Größe der Datenbank hängt vom Aufgabenspektrum / Domänen und Filestruktur-Volumen sowie weiteren Parametern ab.
  Hinweis: bedenken Sie, dass Sie DB Volumen und Anforderungen um Faktor 30 senken können, wenn Sie z.B. das Filesystem nur auf Ordner-Ebene, statt Fileebene auswerten bzw. erfassen.
- Auf dem Installations-Medium finden Sie im Ordner
  \asb Systemhaus\asbLANtools291\Database
  eine fertige, installierbare Datenbank-Dateien vom Typ MDF auf dem Release-Stand 2..9.1 (MS SQL 2008).
  Zur Bereitstellung von „Musterdaten“ für Erstanwender wurde die Funktion zum Einbinden einer MDF Datei als SQL Datenbank in das Modul LTViewer integriert.
- Zum Erstellen einer neuen DB kopieren im ersten Schritt die Datei Muster_<Version>.MDF oder die Demodatenbank (Demo<xy>.MDF) unter dem von Ihnen festzulegenden DB-Namen in das jeweilige lokale SQL-Server-DB Datenverzeichnis.
  Alle weiteren Schritte sind für „Neueinrichtung“ und „Einrichtung Muster-Datenbank“ identisch.
- Im nächsten Schritt müssen Sie die physikalischen MDF Datei an den SQL

Server binden. Dazu bestehen 3 unterschiedliche Optionen:

Einbinden einer DB über SQL Befehl

Das Einbinden einer DB-Datei vom Type MDF in einem SQL Server kann über die SQL Systemfunktion

SP_ATTACH_DB oder die „einfachere“ Variante SP_ATTACH_SINGLE_FILE_DB

Erfolgen, wobei letztere Stored Procedure nur eine MDF Datei einbindet und die sicherste und beste Möglichkeit für das Anlegen einer DB in asbLANtools darstellt..

Dazu verwenden Sie im SQL QueryManager die folgende Eingabe:

Exec SP_ATTACH_SINGLE_FILE_DB ***<log_DB_Name> <physik._MDF_Datei>***

Einbinden einer DB über SQL Manager.

Der mit SQL Server installierbare SQL Manager bietet eine graphische Möglichkeit, SQL Datenbanken in den SQL Server einzubinden. Folgen Sie den Anweisungen im Programm. – Allerdings ist zu bemerken, dass unterschiedliche Releases des SQL Managers bislang hier sehr unterschiedliche Programmoptionen hervorgebracht haben. Wir empfehlen Ihnen deshalb die Anwendung nicht für Anfänger oder SQL unkundige Anwender.

Einbinden einer DB oder Demo-DB über LTViewer.

Eine für asbLANtools Kunden, welche eine Demo-DB oder neue DB nutzen wollen, ist im Modul Viewer die nachfolgende Programmoption entstanden. Diese bietet eine graphische Oberfläche für das verständliche Einbinden einer MDF DB in einen SQL Server.

1. Starten Sie Modul asbLTViewer;
2. Starten Sie unter den Menübefehl „Datenbank“ und dann Auswahl „Datenbank anhängen“. Sie erhalten den folgenden Dialog:
3. Geben Sie den Servernamen des SQL-Servers oder IP Adresse ein;
4. Insofern eine SQL Instanz verwendet wird geben Sie diese ein, andernfalls frei lassen.
   Verbinden Sie Ihre Arbeitsstation zum SQL Server über Button „SQL Server verbinden. Hinweise: Es werden derzeit nur Native Verbindungen unterstützt.
5. Wählen Sie die SQL Datenbank (MDF Datei) zum Einbinden in den SQL Server aus.
   Beachten Sie den Hinweis; Geben Sie, falls der SQL Server auf einem

anderen Server liegt, den „lokalen Ordner“ des SQL Servers ein, der die MDF Datei enthält!

6. Geben Sie den gewünschten logischen DB Namen ein;

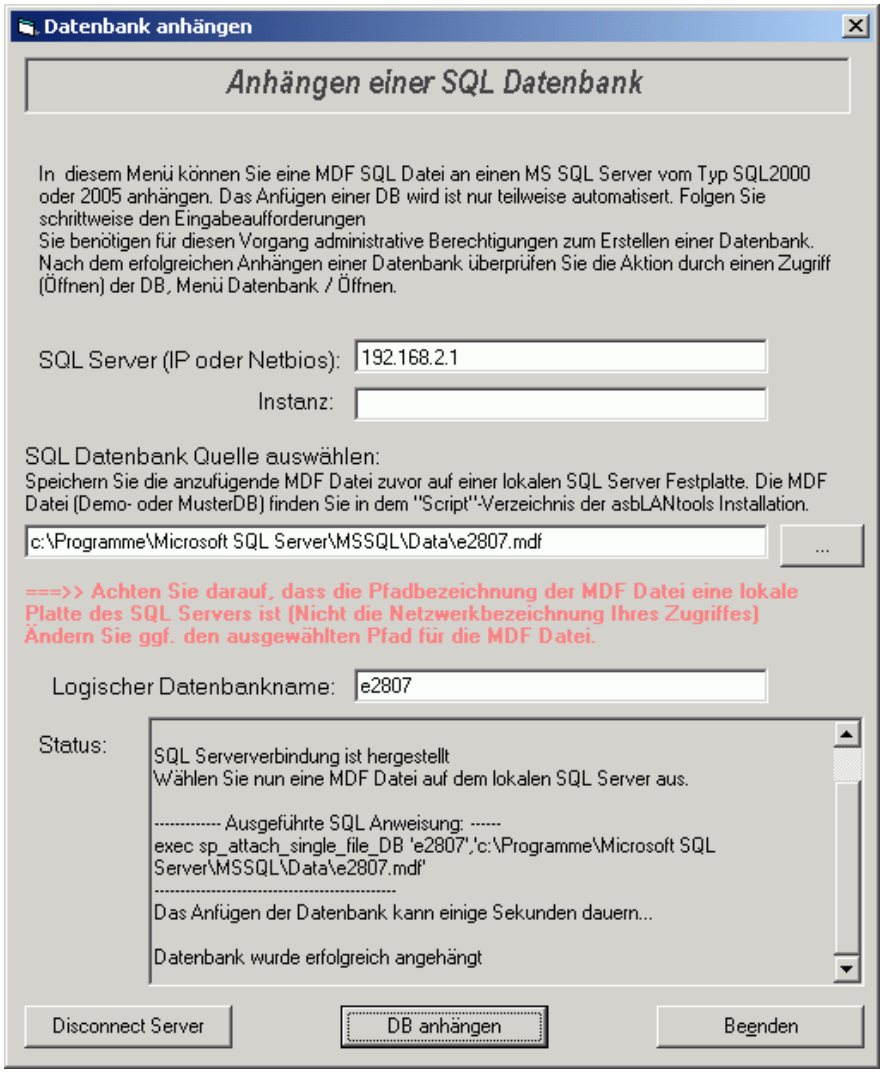

Datenbank anhängen
Anhängen einer SQL Datenbank
In diesem Menü können Sie eine MDF SQL Datei an einen MS SQL Server vom Typ SQL2000 oder 2005 anhängen. Das Anfügen einer DB wird ist nur teilweise automatisert. Folgen Sie schrittweise den Eingabeaufforderungen
Sie benötigen für diesen Vorgang administrative Berechtigungen zum Erstellen einer Datenbank.
Nach dem erfolgreichen Anhängen einer Datenbank überprüfen Sie die Aktion durch einen Zugriff (Öffnen) der DB, Menü Datenbank / Öffnen.
SQL Server (IP oder Netbios):
192.168.2.1
Instanz:
SQL Datenbank Quelle auswählen:
Speichern Sie die anzufügende MDF Datei zuvor auf einer lokalen SQL Server Festplatte. Die MDF Datei (Demo- oder MusterDB) finden Sie in dem "Script"-Verzeichnis der asbLANtools Installation.
c:\Programme\Microsoft SQL Server\MSSQL\Data\e2807.mdf
...
===>> Achten Sie darauf, dass die Pfadbezeichnung der MDF Datei eine lokale Platte des SQL Servers ist (Nicht die Netzwerkbezeichnung Ihres Zugriffes)
Ändern Sie ggf. den ausgewählten Pfad für die MDF Datei.
Logischer Datenbankname:
e2807
Status:
SQL Serververbindung ist hergestellt
Wählen Sie nun eine MDF Datei auf dem lokalen SQL Server aus.
---------- Ausgeführte SQL Anweisung: ------
exec sp_attach_single_file_DB 'e2807','c:\Programme\Microsoft SQL Server\MSSQL\Data\e2807.mdf'
Das Anfügen der Datenbank kann einige Sekunden dauern...
Datenbank wurde erfolgreich angehängt
Disconnect Server
DB anhängen
Beenden

Abbildung 3.3: Datenbank anhängen

7. Betätigen Sie „DB anhängen“.
   Hinweis: Das Einrichten /Anhängen einer SQL DB kann je nach Größe etwas dauern, da die Datei vom SQL Server transformiert wird.
8. Danach können Sie die DB mit Datenbank /Öffnen im Module Viewer oder nach Einrichtung der logischen ADO Datenquelle im Modul Administrator und weiteren verbinden.

Festlegen von Zugriffsberechtigungen

Für den Zugriff auf eine SQL Datenbank ist es erforderlich die Zugriffsberechtigungen festzulegen. Neben administrativen Werkzeugen, können Sie hierzu auch die vorbereitete Rollen-Zugriffsverwaltung nutzen. Informieren Sie sich vorab über Möglichkeiten und Anforderungen. Der MS SQL Server unterscheidet 2 Rollen:

- Datenbank gestützte Rollen
- Applikations- gestützte Rollen

Die Nutzung der Datenbank gestützten Rollen ist sehr einfach für asbLANtools anwendbar. Im SQL Server wird einem eingerichteten Benutzern über die Gruppenzugehörigkeit LT_Reader, oder LT_Writer eine Read / Write Berechtigung zugeordnet. Zum Einrichten der DB Rollen können Sie vorbereitet Skripte nutzen. Dazu gehen Sie wie folgt vor:

- Verwenden Sie ein CD-Konsolen-Fenster;
- Starten Sie CMD> LtAccess.BAT mit den Parametern:
  Parameter-1: Berechtigung: ALLOW / DENY / A / D
  Parameter-2: DB-Server
  Parameter-3: DB-Name
  Parameter-4: Benutzer/Gruppe, für Zugriff
  Parameter-5: asbLANtools Rollen Berechtigung (LT_Reader / LT_Writer / Owner /R /W / O)

Auszug mit Beispiel aus selbsterklärenden Help der BAT Datei:

```
C:\Programme\asbLANtools2.8.0\Skripts\>LtAccess.Bat

•      Prozedur zur vereinfachten manuellen Zuweisung von Benutzerrechten zu einer*
•      asbLANtools Datenbank ueber die DB-Rollen: LT_Reader und /oder LT_Writer   *
•      Voraussetzung: Installierte SQL Client-Komponenten;                        *
•      Aufruf fuer „Benutzer Zugriff erlauben“:                                   *
•      LTAccess.Bat „ALLOW“ (SQL-Server) (LT-DB) (Benutzer/Gruppe) (Rolle)        *

•      Beispiel: LtAccess ALLOW Server1 Lt27_1 asb/Domaenen-Benutzer READ         *
•      Aufruf fuer „Benutzer Zugriff entziehen /verbieten“:                       *
•      LTAccess.Bat „DENY“ (SQL-Server) (LT-DB) (Benutzer/Gruppe)                 *

•      Kurzform-Eingabe: „a“ -ALLOW,
                         „d“ -DENY,
                         „r“ -LT_Reader,
                         „w“ -LT_Writer,
                         „o“ -Db_Owner    *

•      Beispiel: LTAcess a Srv1 Db1 Grp01 o
                         // Erteile Grp01 Db_Owner Recht f³r DB1 auf Srv1*
•                        // DB Serverzugriff muss ggf. manuell entzogen werden,
                         // da noch andere DB Zugriffe bestehen ? *

*Sie koennen die Anweisungen auch manuell ueber OSQL/ Query Man. ausfuehren:  *

•      exec sp_grantlogin ‘user’                                                 *

•      exec sp_GrantDbAccess ‘user’                                              *

•      exec sp_addRoleMember ‘LT_Reader’, ’user’   --bzw.                         *

•      exec sp_addRoleMember ‘LT_Writer’, ’user’                                  *

•      exec sp_addRoleMember ‘DB_Owner’, ’user’                                   *

•      Bzw. fuer Entzug von Zugriff:                                             *

•      exec sp_RevokeDbAccess ,user’                                             *

**** Fertig ***
```

Applikations-Rollen Berechtigungen:

In einigen Fällen kann es erforderlich werden, das für den betrieblichen Datenschutz der Zugriff über Dritt-Anwendungen auf asbLANtools Datenbestände verhindert werden soll (Beispiel Anwender darf mit LTViewer, nicht aber mit SQL Query-Manager auf die DB zugreifen). Dafür können Sie die Einrichtung von Applikations-Rollen des SQL Servers verwenden. Die Einrichtung dieser Rollen ist jedoch nicht Bestandteil der Standardinstallation.

Überprüfung vollständiger DB Strukturen

In jedem Fall sollte nach der Einrichtung einer Datenbank dessen Verfügbarkeit geprüft werden:

- Über Modul Administrator öffnen Sie nach Einrichtung einer Datenquelle (Siehe Einrichten Administrator).
  Prüfen Sie den Schreibzugriff auf eine neu angelegte leere (!) DB, indem Sie Menü „Datenbank/ DB Inhalt löschen“ ausführen.
- Über Modul Viewer öffnen Sie ebenfalls eine Datenbank.
  Nach dem Öffnen prüfen Sie die Menüstruktur (Je nach Inhalt können Sie Unterstrukturen öffnen);
  Über Menü Report starten Sie eine „N“ Report z.B. DB Statistik;
  Reports ohne Inhalt (leeres Ergebnis) teilen dies immer über eine Mitteilungsbox „Dieser Report liefert keine Daten“, oder eine Report-Ansicht mit dem entsprechenden Inhalt mit. In beiden Fällen ist das Report-Interface richtig installiert. Sollte es beim Aufruf eines Reports zu Problemen kommen, müssen Sie für Ihre spezifische Konfiguration eventuell die verwendeten Report Dateien austauschen, da Sie eventuell eine kollidierende Installation auf diesem Rechner besitzen.
  In diesem Fall nutzen Sie die in der Installation befindliche Anweisung und Info-Datei unter „Crystal-Moduls“ zur Fehlerbehebung.
- In anderen Fällen oder bei Fragen wenden Sie sich an Support@asb-systemhaus.de

3.5 Update / Deinstallation

asbLAN*tools* wird mittels Installshield Setup Prozess ausgeliefert.

Dies ermöglicht komplette, individuelle und einfache Installationen der Software. Für eine Neuinstallation/Update der Software sollte diese jedoch zuvor sicherheitshalber deinstalliert werden. Dies vereinfacht den Gesamtprozess.

Ab Version 2.7.0 können mehrere unterschiedliche Programmversionen auf einem Rechner **gleichzeitig** eingesetzt werden. Die Installationsdaten unterscheiden sich dabei an Hand der „Unterversion“ in der Versionsbezeichnung.
Innerhalb einer „installierten Version“ können Bestandteile im Falle einer Korrektur/Update frei ausgetauscht werden.

Die in asbLANtools verwendete Versionsstruktur wird generell nach dem folgenden Prinzip verwaltet (Beispiel: 2.9.1.32):

- Hauptversion 2.9
  Datenbank-Version 2.9.1 => Kennzeichnung DB Modell und Lizenzebene
  Release: 2.9.1.32 => Kennzeichnung Software Stand
- Somit kann neben Version 2.8.0 auch die Version 2.9.1 installiert sein.

- Änderungen innerhalb des Release-Standes können durch einfaches Austauschen der Programm- /Report- und Datendateien erfolgen.
- Datenbank-Strukturen werden innerhalb einer Datenbank-Version nicht verändert.

3.6 Datenübernahme/ Datenarchiv

Mit der stetigen Weiterentwicklung der Software asbLAN*tools* und deren Komponenten und Datenstrukturen treten Fragen zur Kompatibilität / Verwendung früherer Daten auf.

Generell muss diese Frage aus verschiedenen Richtungen betrachtet werden:

- Für die Auswertung bestehender Datenbanken verwenden Sie bitte auch immer die zugehörigen Software (Viewer, Reports und andere). Nur so kann die einfache und dauerhafte Lesbarkeit gewährleistet werden.
- Existierende Altdaten im „Importformat" früherer Versionen können im Allgemeinen problemlos in aktuelle, höhere Versionen von asbLANtools importiert bzw. konvertiert werden. Es kann jedoch zu funktionalen Einschränkungen kommen. Zukünftig wird für Altdaten immer eine Konvertierung in die aktuellen Strukturen angeboten. Importierte Altdaten können zu eingeschränkten Ansichten oder Auswertungen führen (wenn entsprechende Informationen verständlicherweise nicht vorhanden sind).
- Zur Langzeitarchivierung ist es daher zu empfehlen, die jeweiligen „gescannten" Daten und die asbLANtools Software gemeinsam zu archivieren.
- Die aktuelle Version besitzt neben der Möglichkeit 2.9.1 Strukturen auch solche aus 2.8.0 einzulesen.

4 Beschreibung der asbLANtools Module

Die Anwendung der asbLAN*tools* ist grundsätzlich auf Grund des Offline-Konzeptes in 2 Aufgabenbereiche gegliedert:

- Daten-Erfassung (DatenScan)
- Auswertung

Eine Datenerfassung (Scan) von Daten kann mittels der Module

- Administrator
- Modul Batch Prozessor (asbLTcmd)
- Scan- und Import Services

erfolgen. Für die Datenerfassung ist immer eine gültige Lizenz erforderlich. Für die Auswertung und Visualisierung stehen die Module

- Viewer (Visualisierung)
- Report Dokumentation (über den Viewer)
- sowie das offene Datenbankmodell zur Nutzung von Fremd-Software
- zur Verfügung.

4.1 Voraussetzungen

asbLAN*tools* ist als Domänen-Anwendung konzipiert.

Die Software ist somit nur in einer Windows Domänenumgebungen anwendbar. Auswertungen können in beliebigen Umgebungen stattfinden.

Die Datenerfassung von Einzelplatz Rechnern und Arbeitsgruppen wird nicht unterstützt.

Zum Erfassen bzw. Scan von Information sollten mindestens lokale Administrator Privilegien vorliegen.

Für die Erfassung von Informationen (Serverinformationen und deren lokalen Systemeigenschaften) benötigen Sie administrative Rechte.

Beim Aufruf der „Erfassungs-Software“ wird automatisch UAC Control aktiviert, sodass ein Administrator-Account auch mit administrativen Berechtigungen handelt.

4.2 Startmenü

Alle Programmmodule können über die Windows Programmgruppe oder das Startmenü auf dem Desktop aufgerufen werden.

Abbildung 4.1: asbLANtools Startmenü Ikon

Im Startmenü finden Sie auch den Einstieg zur Hilfedatei, Einführung, Lizenzanforderung, sowie zukünftig weiteren Supportunterstützungen.

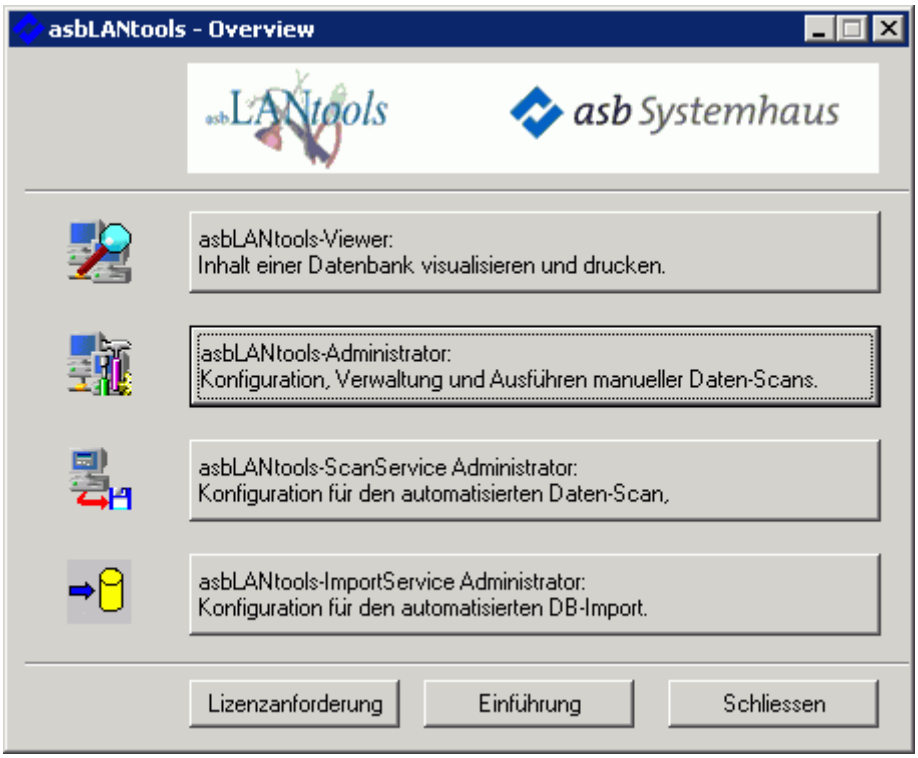


Abbildung 4.2: asbLANtools Startmenü

4.3 Lizenzverwaltung

- asbLANtools Lizenzeingabe
  => Administrator, Menü Extras/Optionen
- Lizenzanforderung
  => Startmenü Schalter „Lizenzanforderung“

4.3.1 Lizenzanforderung

Eine Lizenz für die jeweilige Domäne kann über den Lizenzdialog „Anfordern“ bestellt werden. Dieser Dialog ist auch über das Startmenü asbLAN*tools* unter der Schaltfläche Lizenz zu erreichen.

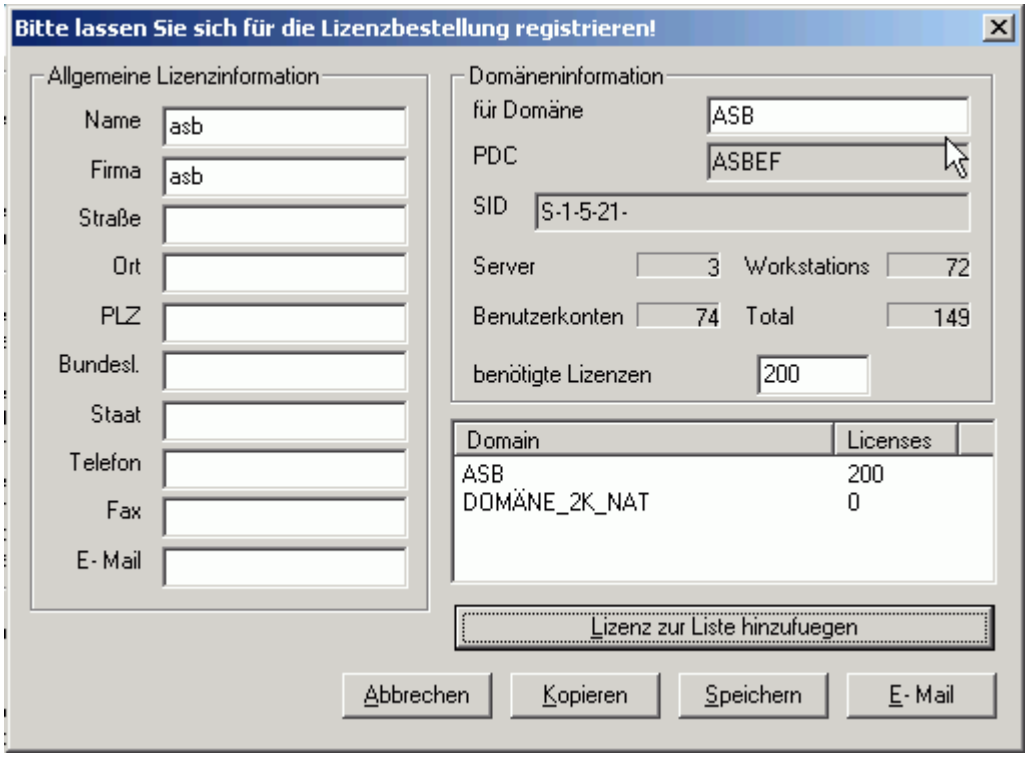


Abbildung 4.3: asbLANtools Lizenz anfordern

Der Dialog Lizenzanforderung ist Ihnen bei der Anforderung einer Evaluierungs- oder Vollversions-Lizenz behilflich.
Senden Sie die Daten als Email oder Faxausdruck.

Informationen zum Lizenzmodell und den von Ihnen benötigten Lizenzen finden Sie unter 3.1.

Mit der Ausstellung einer gültigen Lizenz erhalten Sie eine entsprechende Lizenzdatei vom Typ „*.LIC“. Diese ist auf allen Rechnersystemen, welche Daten mittels dem Administrator, Scan Service oder Batchprozessor erfassen einzuspielen.

Sie können mehrere Lizenzen (für mehrere Domänen) gleichzeitig nutzen.

Neu in Version 2.91 ist, das alle Module eine Lizenz benötigen (auch LTViewer und AD Scan Modul). Die Lizenzgültigkeit für LTViewer wird über die jeweilige Datenbank gesteuert.

4.3.2 Lizenzeingabe

Zu Details der Lizenzverwaltung siehe Kapitel Lizenzanforderung. Die Verwaltung aller Lizenzen erfolgt über den asbLANtools Administrator. Vor dem ersten Einsatz sind notwendige Einstellungen über den Administrator vorzunehmen.

Beim ersten Start des asbLAN*tools* Administrators müssen die Lizenzinformationen eingestellt werden und notwendigen Konfigurationen vorgenommen werden.
Auch für die Evaluierung wird eine Lizenz benötigt.

Mit dem Erstzugriff des Moduls Administrator auf eine Datenbank wird dies auch für Modul LTViewer freigeschaltet.

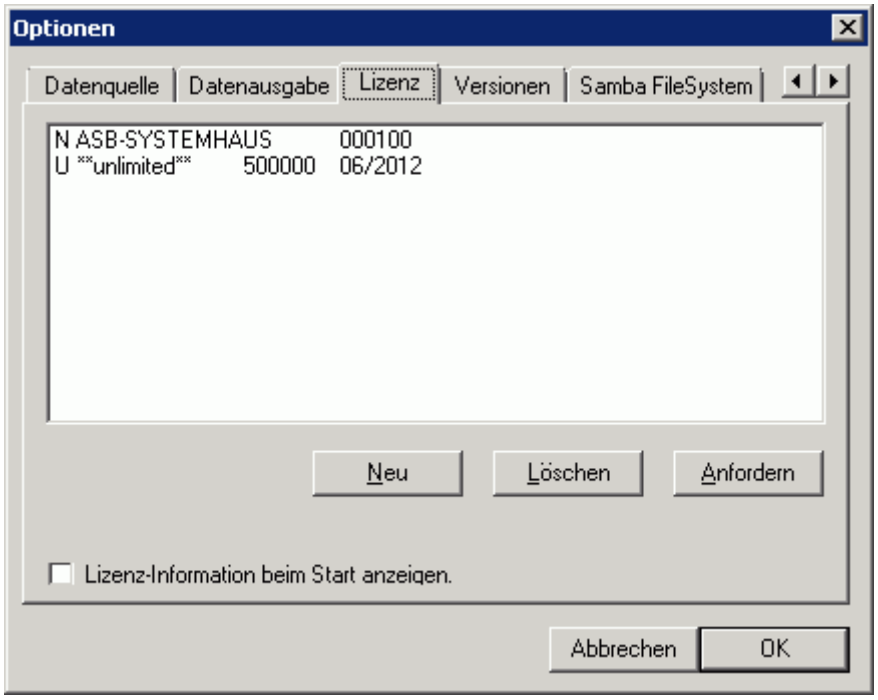


Abbildung 4.4: asbLANtools Lizenzdialog

asbLANtools bietet die Möglichkeit, mehrere, unterschiedliche Lizenzen für Dienstleister zu verwalten.

4.4 Modul Administrator

Der asbLANtools Administrator ist die zentrale Komponente für die Erfassung von Daten im Netzwerk.

4.4.1 asbLANtools Administrator anwenden

Dem asbLAN*tools* Administrator kommt die zentrale Rolle der Kommunikationszentrale für die Datenerfassung zu.

Verwenden Sie als „Einsteiger“ zum Scan von Netzwerkdaten ausschließlich den Administrator.

Der Aufruf des Administrators kann über die Programmgruppe oder das Startmenü, welches mit der Installation auf dem Desktop angeordnet wird, erfolgen.

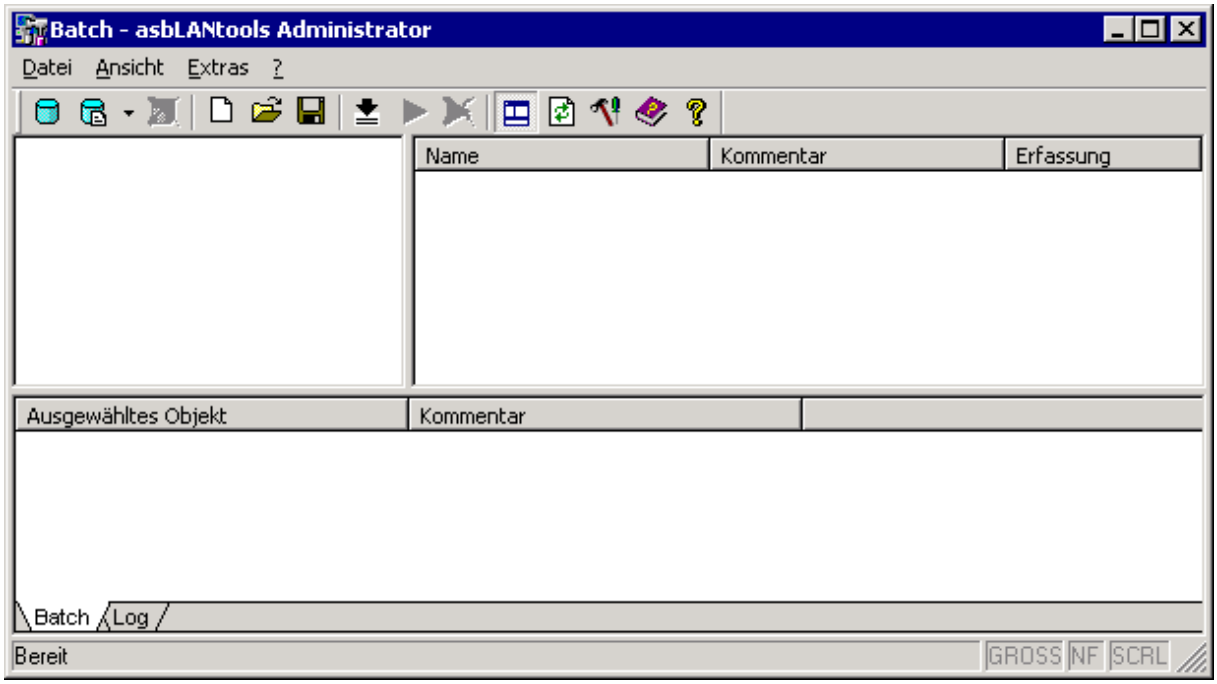


Abbildung 4.5: asbLANtools Hauptmenü

Im ersten Schritt muss eine Datenbank bzw. Datenquelle (bzw. eine Offline-Datenquelle = Dateiablage) zur Speicherung der Scandaten festgelegt werden. Dies erfolgt über das Menü Datenbank öffnen bzw. über das Menü Extras zum Anlegen einer Datenquelle. Im Falle einer SQL Datenquelle werden alle gescannten Daten in einem Verzeichnis zwischengespeichert und von hier in die DB importiert.

Zur Auswahl und Arbeit mit einer Datenquelle lesen Sie auch Kapitel 3.4.

Nach dem Verbinden mit einer Datenquelle erscheint folgende Oberfläche mit der oder den aktiven verfügbaren Domänen und deren Bestandteilen zur Auswahl (Treeview).

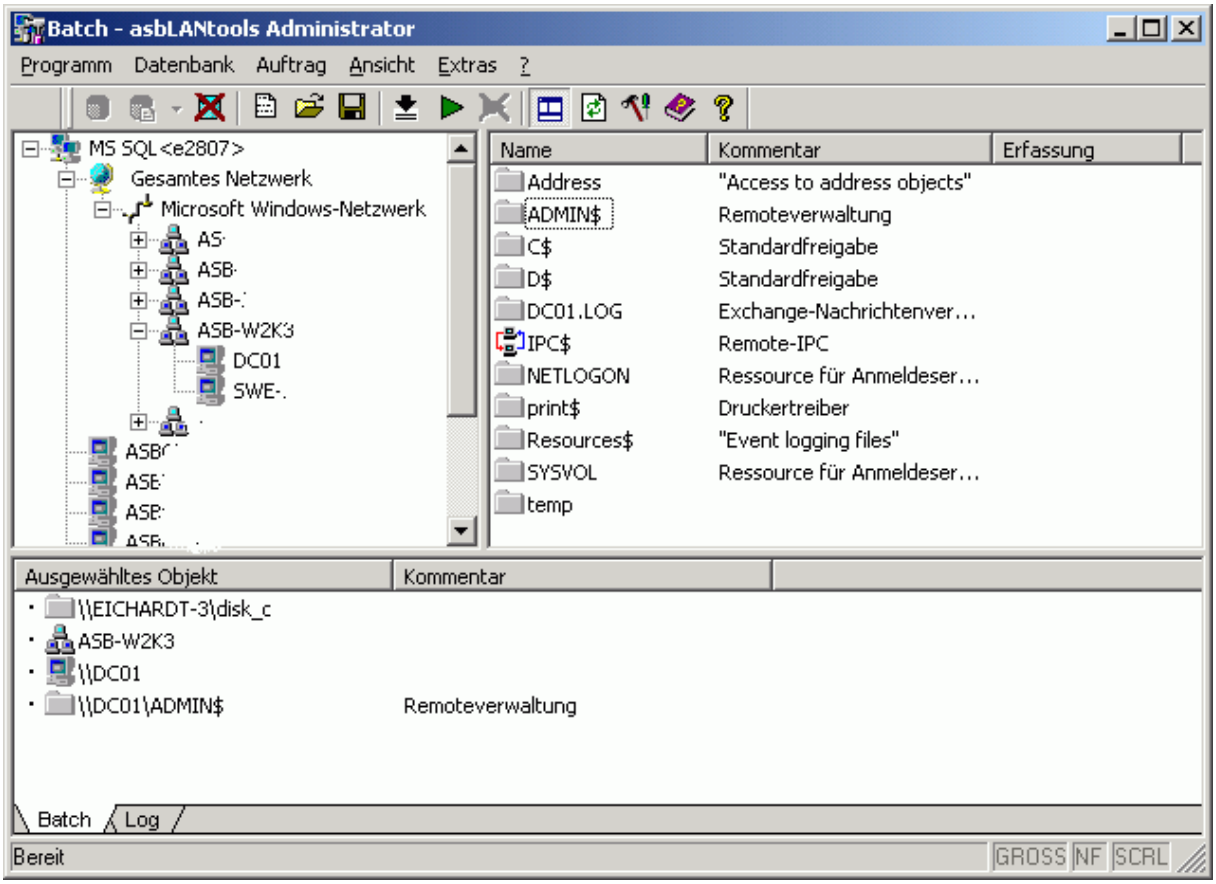


Abbildung 4.6: Administrator Netzwerkansicht

Grundsätzlich ist zum Scan von Informationen zu beachten, dass auswertbare Informationen immer aus der in Rangfolge priorisierten Information:

Domänen:
Zu den Domäneninformationen zählen Benutzerkonten, lokale und globale Gruppen, modale Einstellungen, vergebene Benutzerrechte, Maschinenkonten, sonstige Accounts.

Maschinen:
Lokale Benutzerkonten, lokale Gruppen, Dienste, Drucker und Freigaben sowie Maschinenanmeldedaten in der Domäne (Maschinen-Identifikation).

Dateifreigaben und Verzeichnisdaten:
Zugriffsrechte auf die Dateien und Verzeichnisse in den ausgewählten Freigaben, Fileinformationen inkl. vollständiger ACL und ACE Eigenschaften.

Sie können keine Maschinen und Share- bzw. Fileinformationen auswerten oder anzeigen, wenn die Datenbank keine Domänen Information enthält. Gleiches gilt für Share- bzw. File Informationen, diese bedürfen der zugehörigen Maschinen-Informationen.

Anwendungsspezifische Informationen zum Scannen von Informationen finden Sie in dem Kapitel 0.

Das Scannen der Informationen durch den Administrator oder den ScanService erfolgt auftragsbezogen. Es können mehrere Aufträge bearbeitet werden, jedoch nicht

gleichzeitig auf einer Maschine.

Abbildung 4.7: Auftragsfenster im Administrator

Ein Auftrag wird im Administrator durch den Befehl START ausgeführt und normalerweise mit einer „Ready-Meldung“ und Fehlerstatus im Logfenster wie folgt beendet.

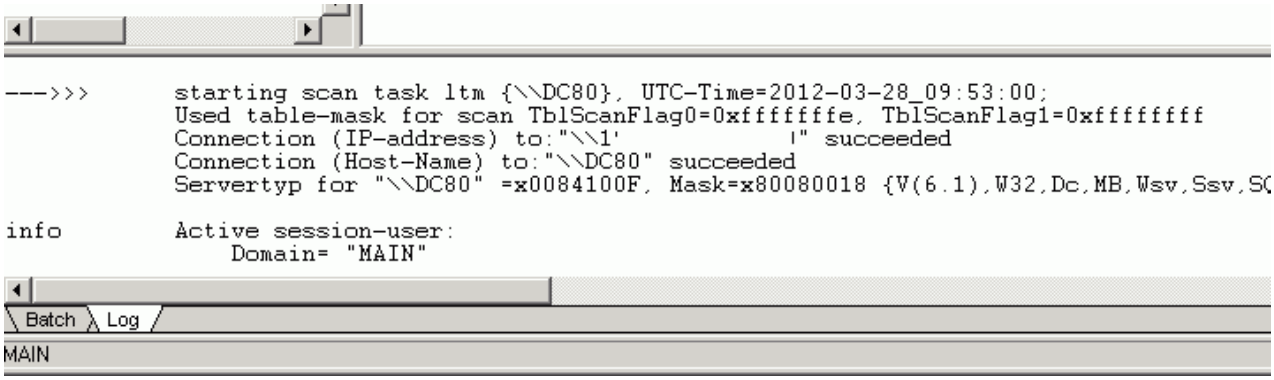


Abbildung 4.8: Logfenster im Administrator

Nach dem Einlesen von Daten in eine Datenbank können ausgewertet werden.
Zum erstmaligen Scan bzw. als asbLANtools Erstanwender verwenden Sie die unter Extras/Optionen eingeschalteten Fehleroptionen. In diesem Fall wird ein vollständiges Log Protokoll über alle Aktivitäten (Scan und Import) im „Log“ Bereich gespeichert.

4.4.2 Datenquellen verwalten

Der in asbLANtools verwendete Begriff Datenquelle kann aus den folgenden Datenquellentypen bestehen:

- SQL Server: MS SQL Server
- Offline Datenquelle (Datenverzeichnis)

Die Offline Datenquelle stellt eine Besonderheit dar und ermöglicht ein DatenScan, auch wenn keine Datenbank zur Verfügung steht. Diese Daten können später über den Menü-Befehl Datenbank/Import direkt in eine Datenbank importiert werden.

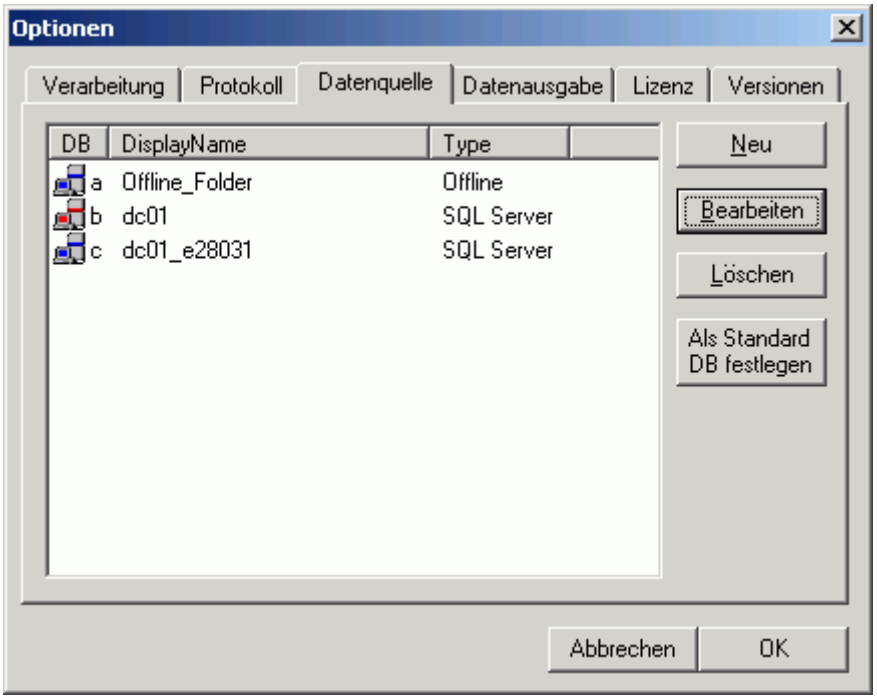


Abbildung 4.9: Datenbankauswahl

Für die Einrichtung einer MS SQL Server werden die Grundkenntnisse eines Datenbank Administrators vorausgesetzt.
Die Nutzung erfolgt anwenderseitig über verfügbare Schnittstellen (ADO, OLE/DB, ODBC u.a.)

Als Standarddatenbank wird die jeweils zugewiesene „aktuelle“ Datenquelle bezeichnet. Beim Datenimport mittels Import Service wird immer in die Standard-DB importiert. Die Standard-Datenquelle können Sie im Administrator oder asbLTcmd.exe Programm für interaktive Nutzung, sowie Import Service für automatischen DB Import zuweisen.

4.4.3 Datenquelle einrichten

Eine neue Datenquelle kann über die folgende Oberfläche angelegt werden.
Eine Datenquelle ist eine logische Zuordnung von Datenbanken oder Offlineverzeichnissen für die asbLANtools Module (Bitte nicht mit ODBC Quellen verwechseln.)

Eine SQL Datenquelle setzt eine eingerichtete Datenbank voraus. Sie können mit asbLANtools beliebig viele Datenbanken verwenden, jedoch immer nur eine Verbindung zu einer Datenbank(Datenquelle) gleichzeitig nutzen.

Zur Einrichtung einer Offline Datenquelle geben Sie bitte ein Datenverzeichnis ein, in welches die gescannten Informationen zu speichern sind.

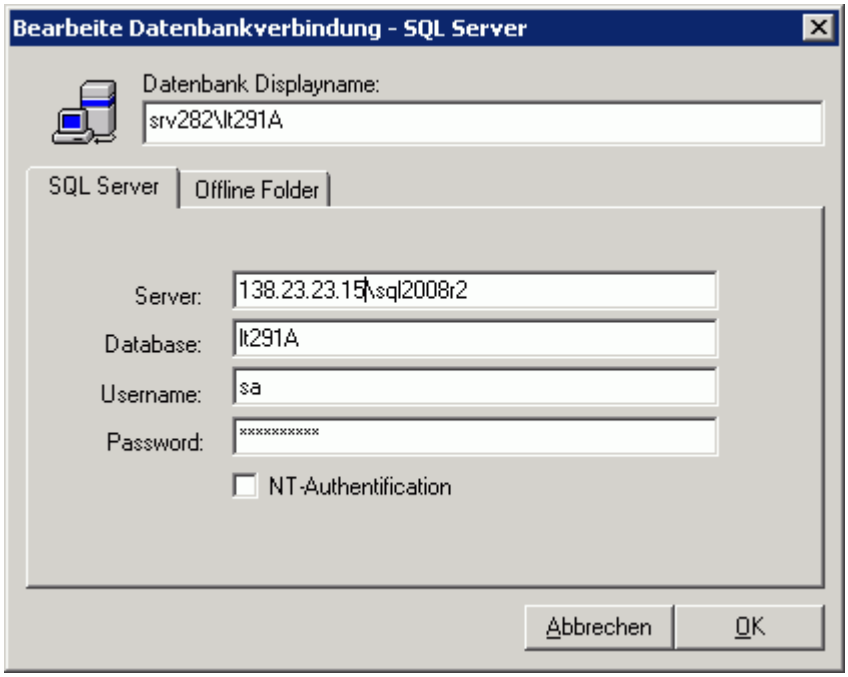


Abbildung 4.10: Zuweisen einer Datenquelle (MS SQL)

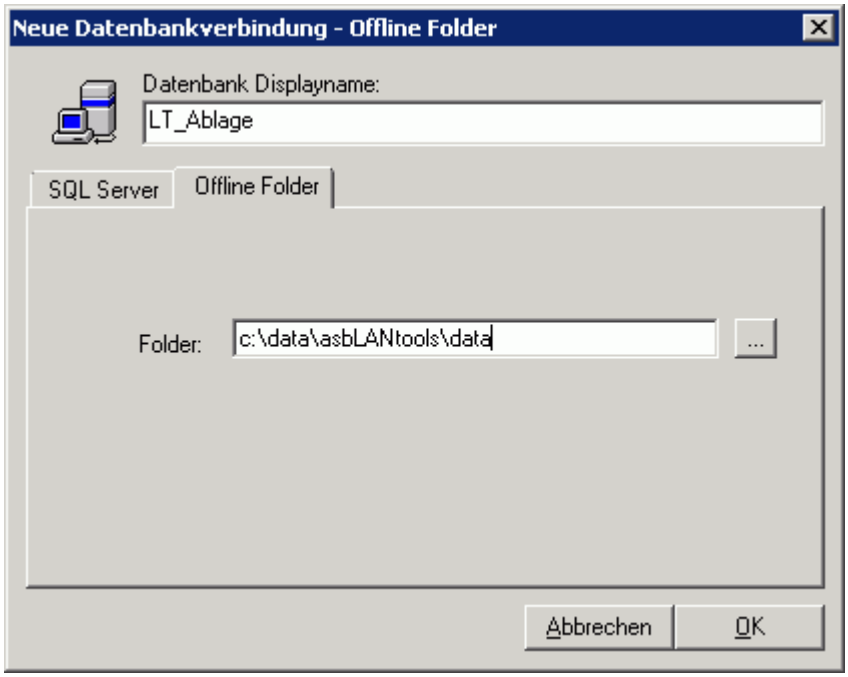


Abbildung 4.11: Zuweisen einer Offline-Datenquelle

Als Displayname geben Sie bitte einen die Datenquelle beschreibenden Namen ein. Bei Zugriff auf mehrerer DB Server fügen Sie bitte den Servernamen zur Identifikation an.

4.4.4 Administrator-Oberfläche im Detail

Der asbLAN*tools* Administrator ist das hauptsächliche Arbeitsmittel zur Erfassung von Daten. Weitere Möglichkeiten bestehen in der Anwendung des Moduls asbLTCmd oder ScanService. Als Neu-Einsteiger sollten Sie ausschließlich den Administrator nutzen.

Nach dem Start des Administrators und dem Verbinden mit einer eingerichteten Datenbank (siehe vorherige Kapitel Datenquellen verwalten) wird die nachfolgende

Oberfläche (siehe Abbildung 4.12) sichtbar: Im linken oberen Fenster F1 wird die Netzwerkstruktur inkl. Maschinen angezeigt.

Im Fenster F2 werden die Details zu selektierten Objekten im Fenster F1 angezeigt. Fenster F3 dient der Auftragsverwaltung (DatenScan und Datenimport) sowie der Darstellung eines Protokoll-Ausschnittes, ca. letzten 100 Zeilen. Ein vollständiges Log-Protokoll finden Sie im „log“ Ordner, oder entsprechend Konfiguration, siehe Menü Extras/Optionen.

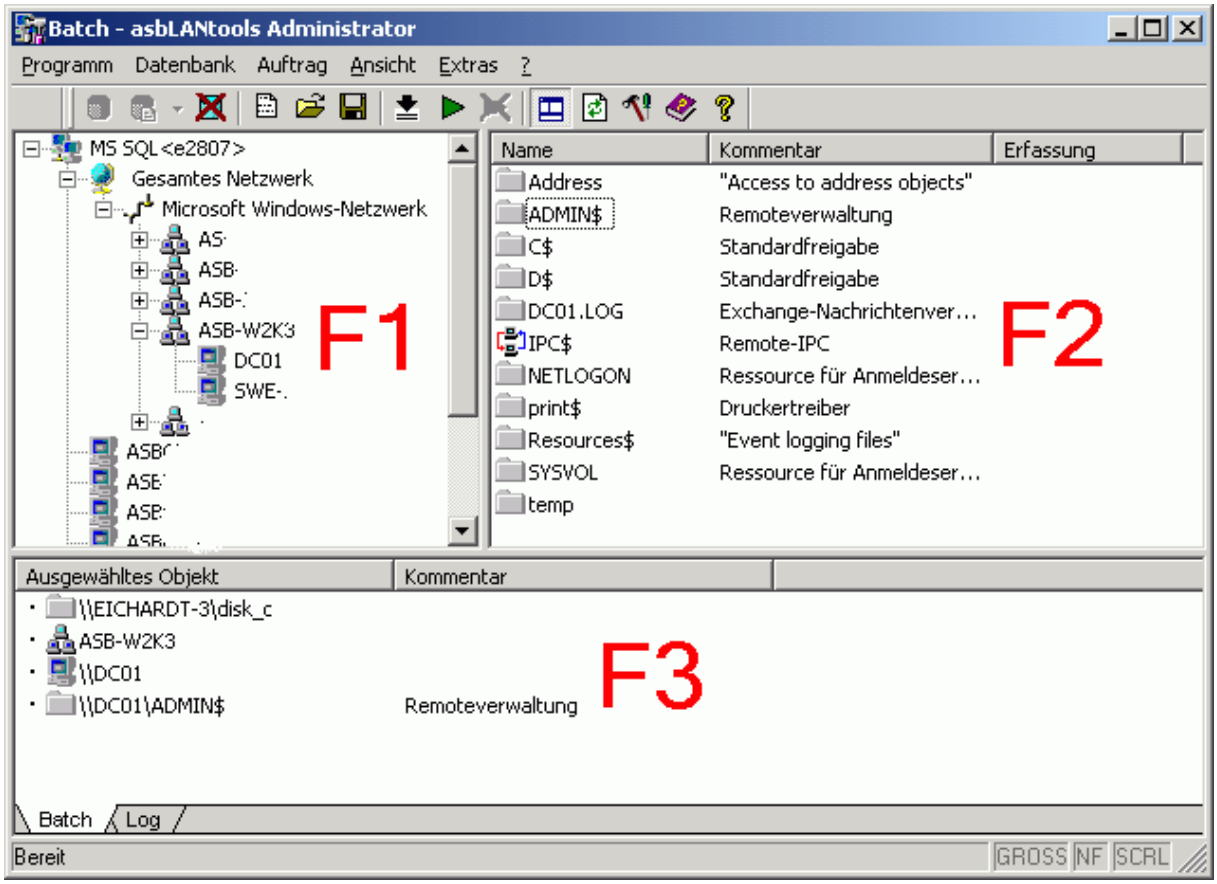


Abbildung 4.12: asbLANtools Administrator

In dem dreigeteilten Bildschirm finden Sie folgende Informationen:

Im Fenster..	.. erfolgt Anzeige von
Fenster F1	Struktur des Netzwerks.
Fenster F2	Detailinformationen.
Fenster F3	Registers „Batch“: zeigt ausgewählte „Auftragsdetails“; Register Logfile: zeigt einen Auszug aus dem Log-Protokoll (letzten Zeilen) an.

Tabelle 4.1: asbLANtools Viewer Fensteraufteilung

Der Administrator besitzt neben den Standard-Menüs zur Steuerung eines Programms folgende wichtige Menü-Befehlsstrukturen:

- Menü Datenbank
- Menü Auftrag

- Menü Extras

Achtung alle Einstellungen im Administrator gelten auch für den Batch-Prozessor asbLTcmd (Speicherung in der Registry). Import- und Scan Service haben separat einstellbare Prozesseinstellungen (Registry).

Der Batch-Prozessor ermöglicht die Erfassung von Informationen auf CMD Ebene. Für den produktiven Einsatz, besonders in größeren Umgebungen sollte der ScanService genutzt werden.

Menü Datenbank

Abbildung 4.13: Administrator Menü Datenbank

- Standard-Datenbank:
  Sie können jede Datenquelle als Standard-DB festlegen. Eine Standard-DB hat ansonsten keinen weiteren wesentlichen Einfluss. Im Modul asbLTCmd wird die Standard-DB als Import-DB benutzt.
- Datenbank Inhalt löschen:
  => Löschen von Informationen aus der aktuellen Datenbank.
  Es können verschiedene Option gewählt werden:

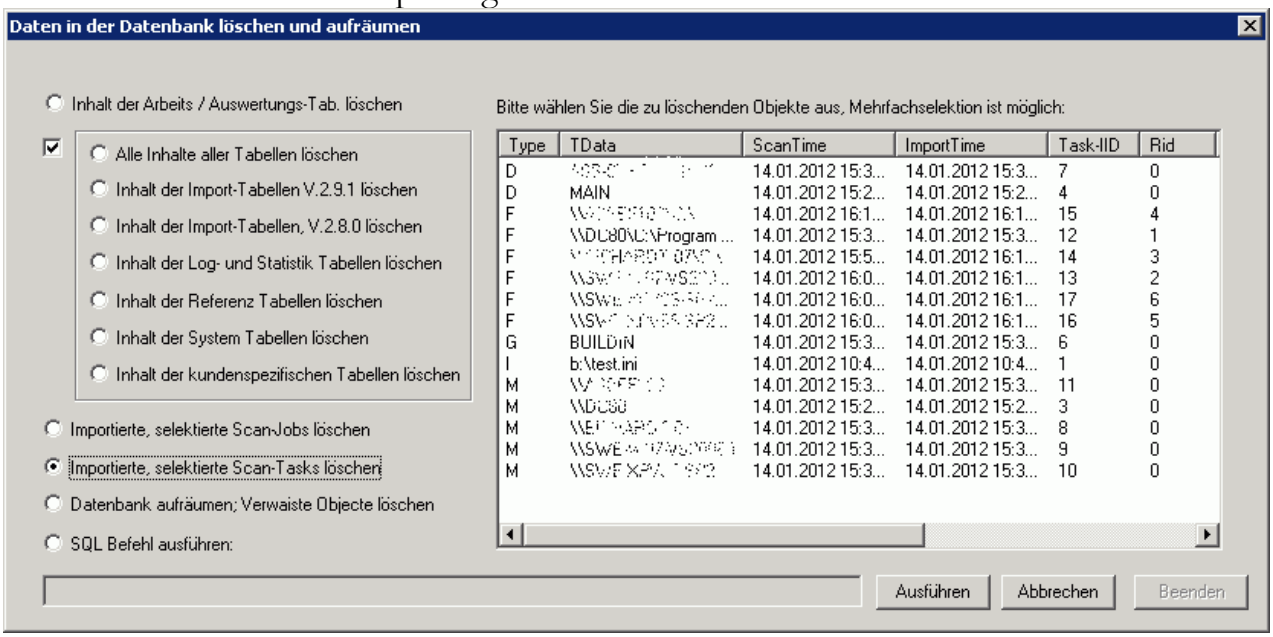

Daten in der Datenbank löschen und aufräumen
Inhalt der Arbeits / Auswertungs-Tab. löschen
Alle Inhalte aller Tabellen löschen
Inhalt der Import-Tabellen V.2.9.1 löschen
Inhalt der Import-Tabellen, V.2.8.0 löschen
Inhalt der Log- und Statistik Tabellen löschen
Inhalt der Referenz Tabellen löschen
Inhalt der System Tabellen löschen
Inhalt der kundenspezifischen Tabellen löschen
Importierte, selektierte Scan-Jobs löschen
Importierte, selektierte Scan-Tasks löschen
Datenbank aufräumen; Verwaiste Objecte löschen
SQL Befehl ausführen:
Bitte wählen Sie die zu löschenden Objekte aus, Mehrfachselektion ist möglich:
Type TData ScanTime ImportTime Task-IID Rid
D 14.01.2012 15:3... 14.01.2012 15:3... 7 0
D MAIN 14.01.2012 15:2... 14.01.2012 15:2... 4 0
F 14.01.2012 16:1... 14.01.2012 16:1... 15 4
F \\DU80\C:\Program ... 14.01.2012 15:3... 14.01.2012 15:3... 12 1
F 14.01.2012 15:5... 14.01.2012 16:1... 14 3
F 14.01.2012 16:0... 14.01.2012 16:1... 13 2
F 14.01.2012 16:0... 14.01.2012 16:1... 17 6
F 14.01.2012 16:0... 14.01.2012 16:1... 16 5
G BUILDIN 14.01.2012 15:3... 14.01.2012 15:3... 6 0
I b:\test.ini 14.01.2012 10:4... 14.01.2012 10:4... 1 0
M 14.01.2012 15:3... 14.01.2012 15:3... 11 0
M \\DU80 14.01.2012 15:2... 14.01.2012 15:2... 3 0
M 14.01.2012 15:3... 14.01.2012 15:3... 8 0
M 14.01.2012 15:3... 14.01.2012 15:3... 9 0
M 14.01.2012 15:3... 14.01.2012 15:3... 10 0
Ausführen
Abbrechen
Beenden

Abbildung 4.14: Administrator Dialog Datenbank löschen

- DB Statistik:
  => Anzeige einer Übersicht der zur Datenbank gehörigen Tabellen und dessen Inhalte. Ausführliche Aussage zu DB Inhalten können über Report N9 sowie über Ansichten im Modul asbLTViewer erreicht werden. Für SQL kundige Anwender besteht die Möglichkeit SQL-Instruktionen im Module asbLTViewer/ QueryManager direkt an eine DB zu senden, falls keine anderen SQL Werkzeuge verfügbar sind.

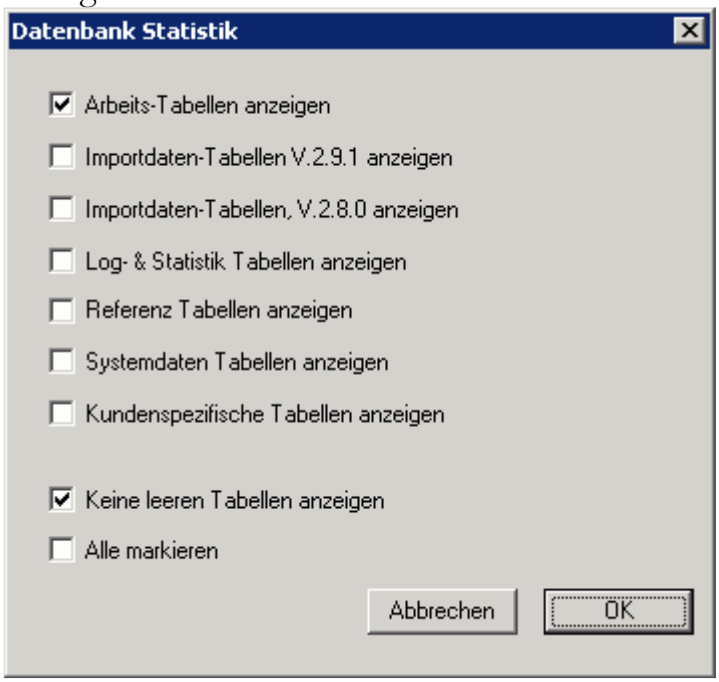


Abbildung 4.15: Administrator Dialog Statistik

Menü Auftrag

Der Auftragsdialog enthält Befehle zur Erstellung und Ausführung eines Auftrages zum

- DatenScan und
- Datenimport in eine Datenbank.

Ein Auftrag kann als Auftragsdatei gespeichert und mitteln eines Texteditors bearbeitet werden.

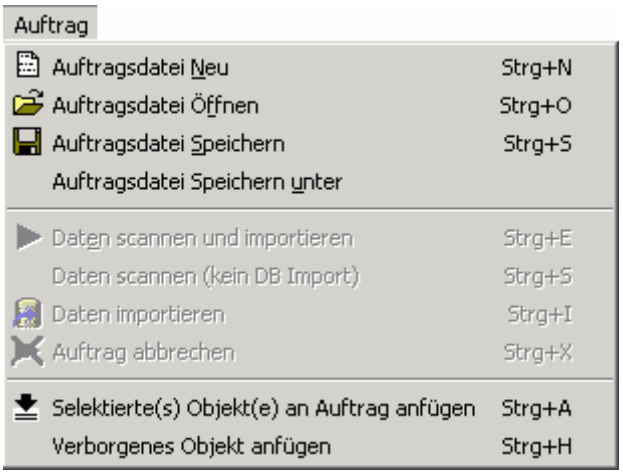


Abbildung 4.16: Das Menü Auftrag

- Ein Auftrag (Job) auch als Batch bezeichnet besteht aus einem oder mehreren einzelnen Anweisungen(Tasks) zum DatenScan und Datenimport. Alle Aktivitäten der Auftragsverarbeitung werden in einem Log-Protokoll nachvollziehbar (siehe Log) unter einer eineindeutigen Job- und Task-Nummer gelogged. Ein Logeintrag enthält alle wichtigen Prozess- und teilweise Daten-Logs einer Task. Die Informationen können manuell (bis auf Fehlerebene) reduziert werden.
- Auftragsdatei Neu/Öffnen/Speichern.. dienen der Verwaltung einer Auftrags-(Job) Datei, bestehend aus mehreren einzelnen Aufträgen (Task).
- Selektiertes Objekt an Auftrag (Batch) anfügen:
  Manuelles Hinzufügen eines selektierten Elementes zu einem Auftrag im Register Batch. Als weitere einfache Möglichkeit können Sie auch die Drag & Drop Technologie anstatt des Menü-Befehles „Anfügen“ verwenden.
- Verborgenes Objekt anfügen
  Sofern nichtverfügbare /unsichtbare Rechner und Details zum Auftrag zugefügt werden sollen, kann diese über die Auswahl in diesem Menü erfolgen.
  Die fehlende Anzeige von Domänen, Maschinen und Freigaben kann unterschiedliche Ursachen haben.
  Über eine verdeckte Freigabe lassen sich auch Teile einer Freigabe als Auftrag für ein DatenScan eingeben.
- Eingabe IP Adresse oder NetBios Name:
  Sie können anstatt des NetBios Namens für Maschinen auch die IP- Adressen benutzen.

Menü Extras/ Optionen

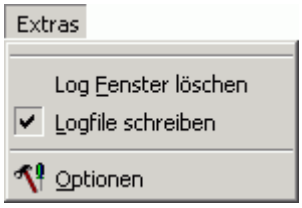


Abbildung 4.17: Das Menü Extras

Über das Menü „Extras“ können notwendige Einstellungen vorgenommen werden:

- Log Fenster löschen:
  Löschen aller Informationen aus dem Log Fenster
- Schreibe Protokolldatei:
  Option aktiviert/ deaktiviert die Protokollierung in einer Logdatei; einstellbar unter Extras/ Optionen/ Verarbeitung.
- Optionen:
  Untermenü Optionen wird ausgewählt, siehe auch Abbildung 4.18.

Im Menü Extras/ Optionen sind verschiedene Kartenreiter (Register) für die Bearbeitung von Einstellungen wählbar, welche im Folgenden näher erläutert werden.

Menü Extras/Optionen/Verarbeitung

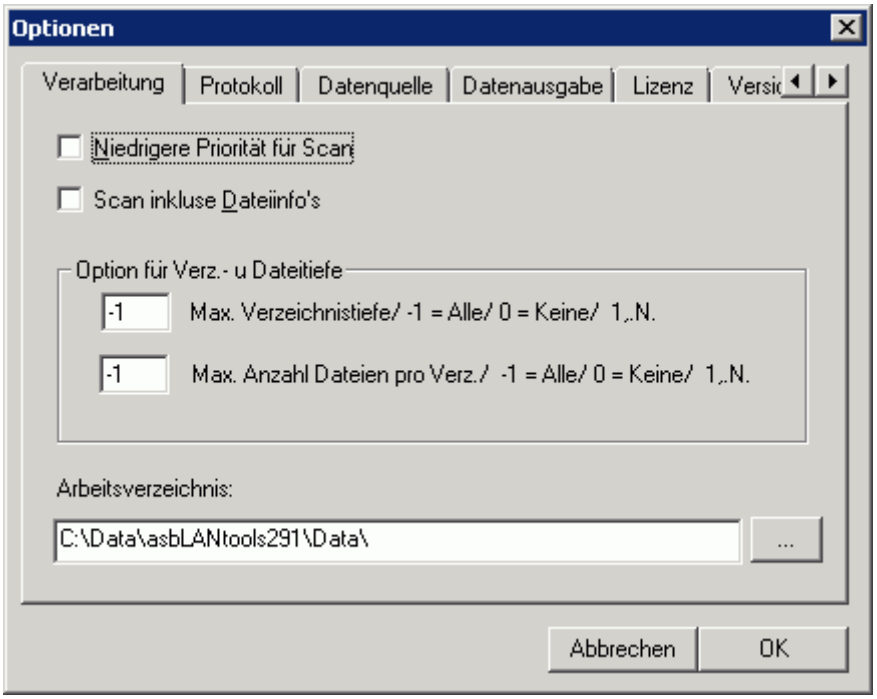


Abbildung 4.18: Dialog, Verarbeitung

- Niedere Priorität:
  Ermöglicht eine Reduzierung der CPU-Belastung. Der Prozess nutzt „freie“ Ressourcen. Die Interaktion zu anderen Programmen wird während der Laufzeit verbessert.
- Scan inklusive Dateiinformationen:
  Der Scan von kompletten Verzeichnisbäumen ist der CPU- und Ressourcen-aufwendigste Prozess. Eine Minimierung nicht benötigter Daten ist somit für die Scanzeit von Vorteil. Fileinformationen werden beim Datenimport verdichtet. Die Option „Inklusive Dateiinformation“ erfasst alle Daten zu Dateigröße, wenn ansonsten keine Files gescannt werden (Zur Übersicht der Ordnergrößen).
- Elternobjekte sammeln älter als x Tage:
  Die Einstellung (Standard 7 Tage) ist eine Hilfe für vergessliche Benutzer.
  Beim Scan eines Dateisystems ist zur Auswertung die Maschinen- und die Domäneninformation erforderlich.
  Option „inklusive D.I“ steuert das Anfügen einen Objektes im Bereich „Batch“.
  Ist ein abhängiges Objekt länger als x Tage nicht gescannt worden, schlägt es durch Zufügen der abhängigen Objekte den Scan dieser Objekte vor. Sie können den Wert mit „0“ ausschalten.
- Arbeitsverzeichnis:
  Dieses Arbeitsverzeichnis wird als temporärer Datenspeicher benutzt.
- Max. Verzeichnistiefe:
  Diese Angabe regelt beim Verzeichnisscan die Tiefe der Verzeichnisstruktur.
  Einstellung -1 scannt alle Verzeichnisse, 0 nur das Wurzelverzeichnis;
- Max. Files:
  Legt die Anzahl je Verzeichnis zu scannenden Dateien fest.
  Standard = 3, 0 keine Verzeichnisse -1 alle Verz. scannen

Menü Extras/Optionen/Protokoll

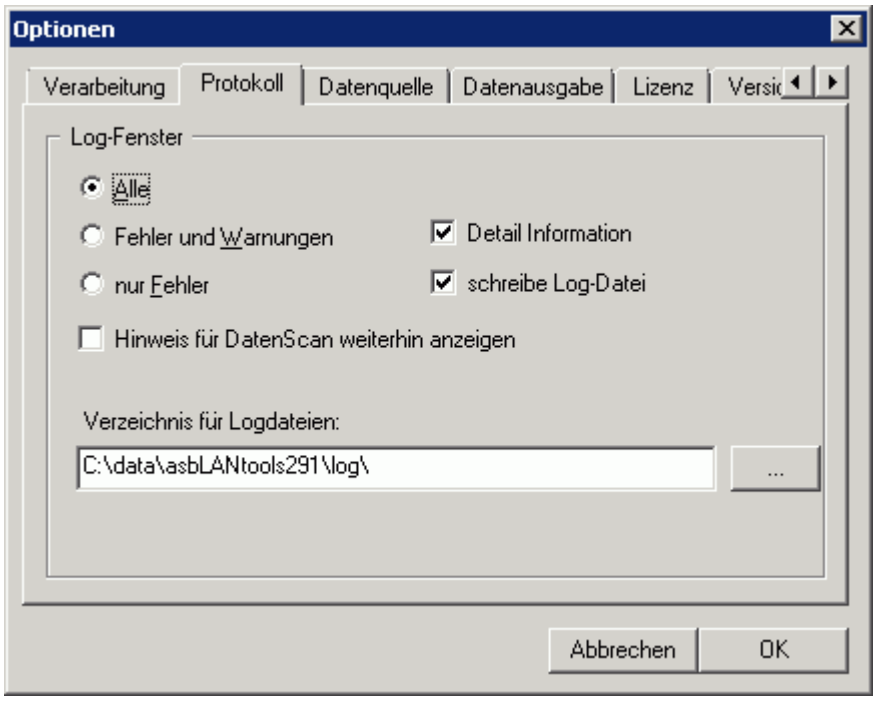


Abbildung 4.19: Dialog Protokoll

Es können verschiedene Optionen für ein Logfile festgelegt werden.
Option „Pause bei Fehler“ unterbricht die Dialog-Abarbeitung im Falle eines Fehlers.

Die Auswahl Log-Fenster ermöglicht die Selektion der auszugebenden Informationen während des Erfassungsprozesses. Wird ein Häkchen bei Detail Informationen gesetzt, dann werden diese während des Erfassungsprozesses im Administrator ausgegeben. Ein Unterbrechen bei Fehlern ermöglicht die Option „Pause bei Fehler“.

Die Option Detailinformation bewirkt eine ausführliche Protokollierung.

Menü Extras/Optionen/Datenquelle

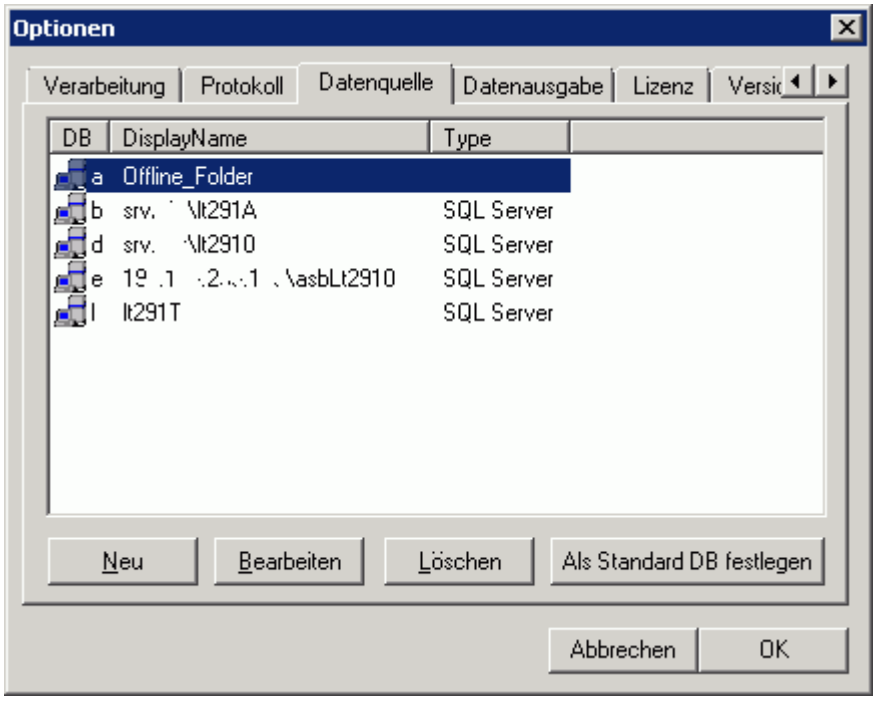


Abbildung 4.20: Dialog Datenquelle

In diesem Dialog können die Datenbanken eingerichtet werden. Weitere Informationen finden Sie im Kapitel Datenbanken.

Menü Extras/Optionen/Datenausgabe

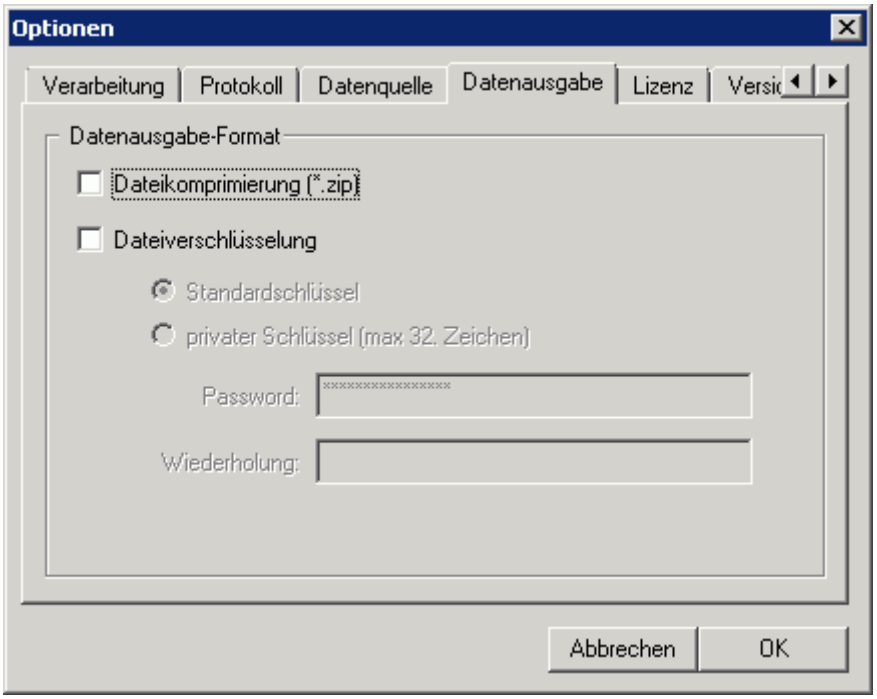


Abbildung 4.21: Dialog Dateiübertragung

- Dateikomprimierung:
  Die Verwendung der Gnu-Zip Komprimierung ermöglicht eine starke Reduzierung der Scandaten.
  Die Scandaten werden aus dem Erfassungsprozess verdichtet abgelegt.
  Die Aktivierung einer Dateiverschlüsselung stellt einen minimalen Datenschutz während der Übertragung der Scandaten dar.
  Scandaten sollten als „gesammelte Security Informationen“ in jedem Fall gesichert gespeichert, transportiert und übertragen werden.
- Dateikomprimierung:
  Die Ausgabedateien werden mit GnuZip um ca. Faktor 6 bis10 komprimiert. Die Daten sind mit Zip Reader lesbar, oder mit dem beiliegenden Serviceprogramm Gzip.Exe (originalgetreu) lesbar /behandelbar.
- Privater Schlüssel:
  Verwenden Sie diese Option nur, wenn Sie a) gescannte Daten vor unbefugten Benutzern sichern müssen und b) notieren Sie sich das Password sicher.
  Eine Decryptierung der Daten ohne Password ist nicht möglich. Ferner benötigen Sie dieses für einen späteren Import gescannter/cryptierter Daten.

Menü Extras/Optionen/Lizenz

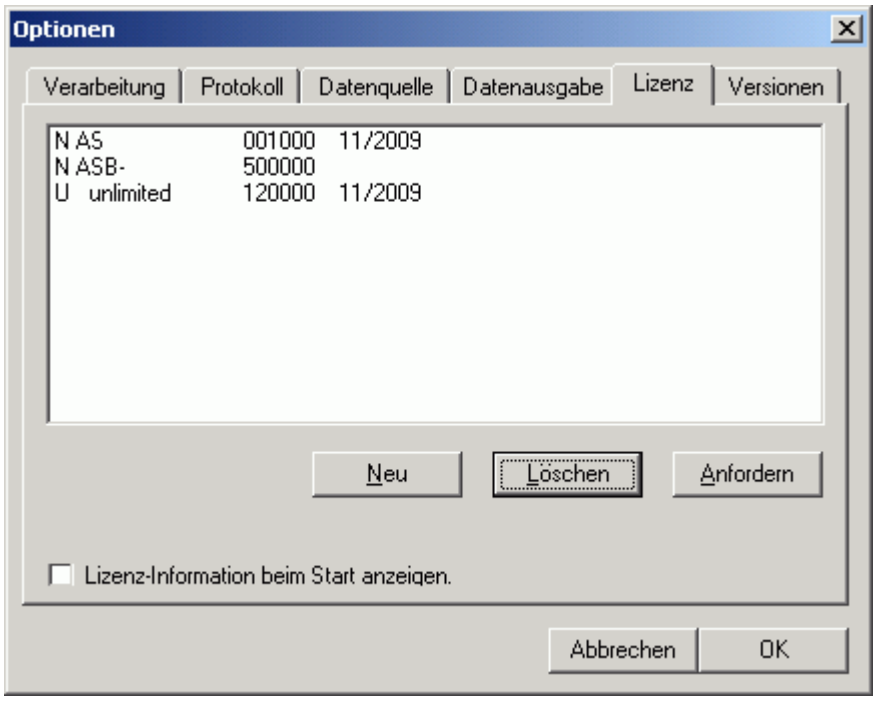


Abbildung 4.22: Dialog Lizenz

Die aktuelle Lizenz wird in diesem Dialog angezeigt. Es besteht die Möglichkeit eine neue Lizenz einzutragen oder anzufordern bzw. eine bestehende zu löschen.

Menü Extras/Optionen/Versionen

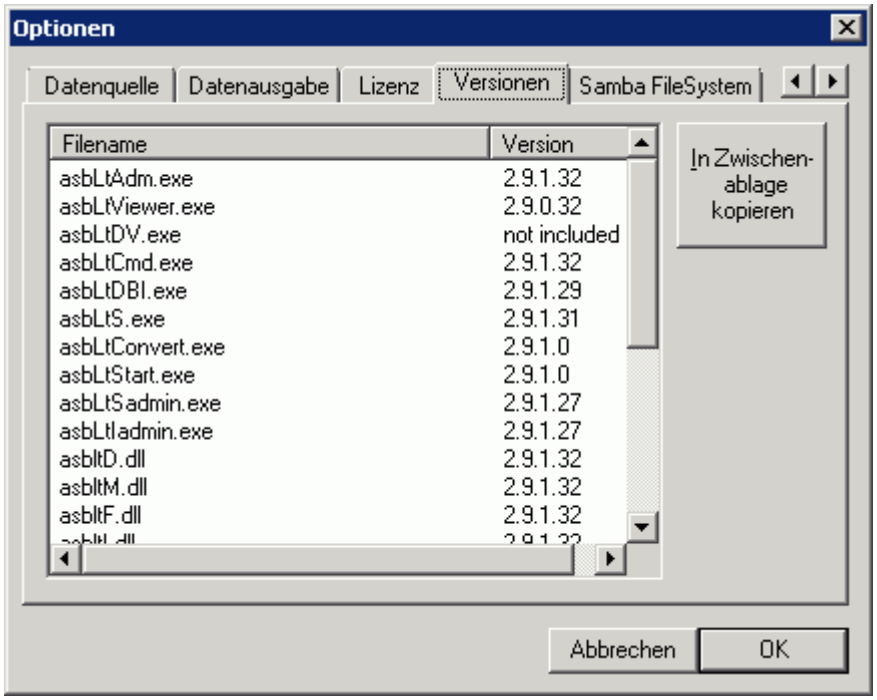


Abbildung 4.23: Dialog Versionen

In diesem Dialog werden die wichtigsten Dateien mit der dazugehörigen Version angezeigt. Über den Button „Zwischenablage“ ist es möglich die hier dargestellten Informationen in die Zwischenablage zu kopieren.

4.4.5 Objekte für ein DatenScan auswählen

Sie können nun durch Auswahl der verschiedenen Objekte steuern, welche Informationen erfasst werden sollen. Um ein Objekt in den Erfassungsauftrag aufzunehmen, haben Sie drei Möglichkeiten:

Sie können den Befehl „an Batch anfügen“ aus dem Kontextmenü verwenden, nachdem Sie das Objekt markiert haben.

Sie können das Objekt einfach mit der Maus in das untere Fenster des Bildschirms ziehen. Die asbLAN*tools* unterstützen Drag and Drop Funktionalität.

Sie können das Symbol in der Symbolleiste anklicken, nachdem Sie das Objekt markiert haben.

Mehrfachselektionen können durch Windows-konforme „Strg“ oder „Umschalt“-Taste“ gesteuert werden.

Nicht sichtbare Objekte können über den Menüpunkt „Extras – Verborgenes Objekt“ angefügt werden.

Hilfreich ist auch die Eingabemöglichkeit über eine IP-Adresse. Sie können sowohl Share/Maschine als auch die Domäne über einen DC-Controller über IP-Adresse auswählen.

Ausgewählte Objekte eines Auftrages werden im Auftragsfenster („BATCH“) sichtbar:

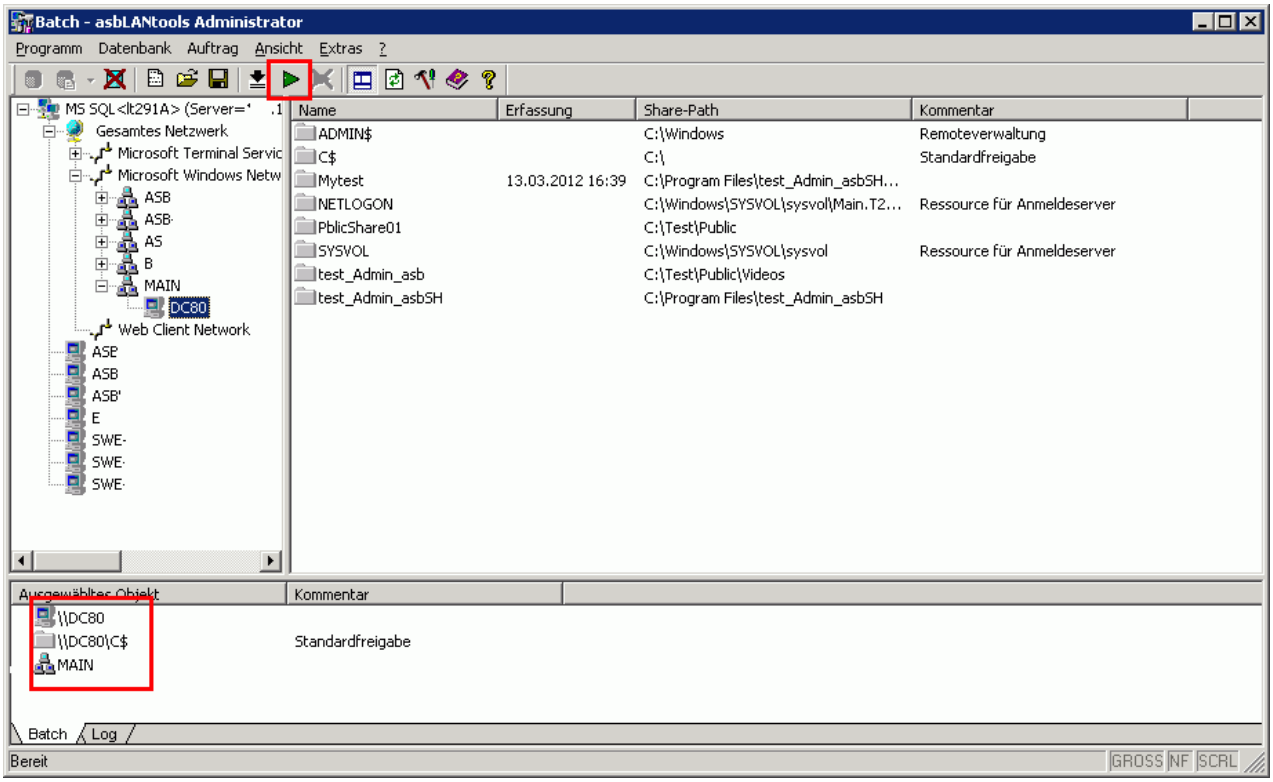


Abbildung 4.24: Administrator Oberfläche

Einen Auftrag im „BATCH“ Fenster bestehend aus mehreren Objekten kann als „Auftragsdatei vom Typ <.LTB> (Standard-Textdatei) zur Wiederverwendung bzw. automatisierten Verarbeitung mittels ScanService gespeichert werden (Menü Auftrag). Den Aufbau der <.LTB> (Auftrags-) Datei finden Sie im Kapitel 4.10.1. .

Das Ausführen eines Scan Auftrages im Register Batch wird über den Befehl „Batch Ausführen“ oder alternativ auch über das Symbol in der Symbolleiste aktiviert.

Scan-Aufträge können alternativ über den Batch-Prozessor oder ScanService verarbeitet werden.

Während der Ausführung des Erfassungsprozesses wird im Logfenster/ Register <LOG> des unteren Bildschirmbereichs der aktuelle Protokollausschnitt angezeigt. Dieses kann optional in einer Logdatei gespeichert werden.
Die Beendigung eines Auftrages wird immer für jedes „Auftragselement“ sowie den gesamten Auftrag mit Angaben der Laufzeit und Fehleranzahl angezeigt.

Ausführliche Fehlernachrichten sind im Logprotokoll ersichtlich. Insofern Fehler auftreten kann das Protokoll nach dem Textstring „Error“ durchsucht werden. Der Fehlerstatus wird immer im Status eines Logeintrages (erste 12 Zeichen) gekennzeichnet. Fehlerhafte, bzw. erfolgreiche Ausführungen werden durch Symbole dargestellt.

Für den produktiven Einsatz von Scan- und Importaufträgen sollten Sie den Scan- und ImportService oder auch den asbLTcmd Prozessor für „kleinere Umgebungen“ verwenden.

Beispiel einer Auftragsdatei:

```
D Domäne01          // Domäne über NetBios Name auflösen und scannen
D 192.109.100.1     // Domäne über IP auflösen und scannen
M \\192.109.100.1   // Maschinen Informationen über IP Adresse scannen
M \\dc01            // Maschineninformationen DC01 scannen
                    // Eine Maschineninformation beinhaltet kein Filesystem!
F \\192.109.100.1}c$ // Filesystem C$ der Maschine 192.109.100.1 über IP
                    // Verbindung auflösen und scannen.
F \\DC01\D$         // Disk D$ der Maschine DC01 über NetBios auflösen
                    // und scannen.
```

4.4.6 DatenScan Prozess

Der DatenScan innerhalb einer Domäne ist meistens unspektakulär. Voraussetzung ist das der Benutzer zum Datenerfassen Domänen-Admin Berechtigungen, bzw. mindestens Administrator Berechtigungen für eine Standortdomäne besitzt. Nicht analysierbare Konten und Daten auf Grund fehlender Berechtigung werden als Warnung oder (insofern zwingend erforderlich) als Fehler im Protokoll ausgegeben. Analysieren Sie beim ersten Scan immer das Logprotokoll.

Die Auflösung eines zu scannendes Objekts (Domäne/Maschine/Filesystem) erfolgt über IP Adresse (s.o.) oder NetBios Auflösung.
Für den Zugriff (Scan) eines Objektes sind meistens (je nach Optionen, Netzwerkkonfiguration u.a. Werten) IP Verbindungen erforderlich. Zu einem entfernten Netzwerk/Domäne /Teildomäne haben Sie nicht automatisch eine IP basierende Verbindungen, sondern meistens „NetBios über IP“.
Insofern ist es bei manuellen Verbindungen erforderlich, dass Sie eine IP basierende IPC$ Verbindung, neben der IPC-NetBios Verbindung zu öffnen. Dazu bietet sich über CMD Schnittstelle folgende Möglichkeit:

Net Use \\<ip-adresse>\IPC$ /User:<Domäne>\<User> /Password:<Password>

Für IP-Adresse, User und Password, müssen Sie Ihre Verbindungsdaten eingeben. „<Domäne>“ ist immer die „Zieldomäne“ des Anmeldeservers.

Entscheidend für eine fehlerfreie Objekt- /Netzwerkkennung ist eine funktionierende DNS Auflösung. Ebenfalls treten mitunter Active Directory Probleme bei Vorhandensein mehrerer AD Server, an verteilten Standorten und fehlerhafter Synchronisation auf. Prüfen Sie in diesem Fall die Informationen im Logfile sorgfältig. Ggf. erhalten Sie hier durch asb Systemhaus Support.

4.4.7 Scannen von nicht- Windows konformen Servern

Als nichtkonforme Systeme werden Systeme bezeichnet, welche unvollständige Informationen auf Standard-Netzwerk-API Anfragen liefern. Diese Systeme sind in der Praxis durchaus weit verbreitet, zumal für eine Datenanalyse wie mit asbLANtools wesentlich mehr und ausführlichere Informationen zu erfassen sind, als Sie im Normalfall bei Zugriff auf ein derartiges System (meistens Datenspeicher .. UNIX basierende externe Systeme) im ersten Anschein vorfinden.

Mit asbLANtools wird die Windows basierende Domänenkennung seitens der eingebundenen Geräte gefordert. Dies ist erforderlich, um eine einwandfreie Aussage zu Berechtigungen zu treffen.
Anbei die häufigsten Probleme und deren Umgehungslösung:

- Fehlerhafte Domänenkennung von „nicht Windows konformen Systemen“:
  In diesem Fall haben Sie die Möglichkeit für eine Maschine einen DC festzulegen. Dazu tragen Sie manuell in der Registry unter HKLM/Software/../asbLANtools291/PredefServers
  einen neuen Untereintrag für den NetBios Maschinennamen in der Domäne und den Eintrag „DC=<DC-Adresse>“ (IP oder NetBios) ein.
  (Ein Mustereintrag ist mit Installation vorhanden)
- Fehlerhafter Cluster Kennung:
  Nutzen Sie für den DatenScan in diesem Fall einen Zugriff auf die realen Maschinen. Ursache meistens eine falsche temporäre Auflösung durch eine API.
- DFS Kennung falsch:
  asbLANtools beherrscht zur Erfassung von Filesystemen auch neben Shares die Erfassung über DFS. Nicht immer ist die DFS Kennung über einen UNC Stream sauber analysierbar. Treten Analyseprobleme auf, nutzen Sie die „verlängerte“ Eingabe über eine Root-Disk. Unter „verlängerter“ Eingabe ist die Eingabe von Unterverzeichnissen in der Share-Eingabe zu verstehen (Beispiel „C$\Temp“ Unterverzeichnis Temp im Verzeichnis C$, anstatt \\Temp Share oder DFS.

Aus datenschutzrechtlichen Gründen werden hier keine nicht-konformen Systeme genannt.

4.4.8 Protokollierung

In allen Programm Modulen wird eine ausführliche, einstellbare Protokollierung erstellt. Für „neue“ Anwender und unbekannte Umgebungen empfiehlt sich, alle Protokolloptionen einzustellen Menü Extras/Optionen/Protokoll.

Im Administrator wird das Protokoll sowohl für eine schnelle Kontrolle im Fenster Log dargestellt, als auch in seiner Gesamtheit als Logdatei unter dem jeweiligen Job Namen mit Ident-Nummer im Ordner DATA gespeichert.

Für jeden Abschnitt der Verarbeitung eines Auftrages (Job) erfolgt eine übersichtliche Darstellung, hier anbei Scan einer Maschine:

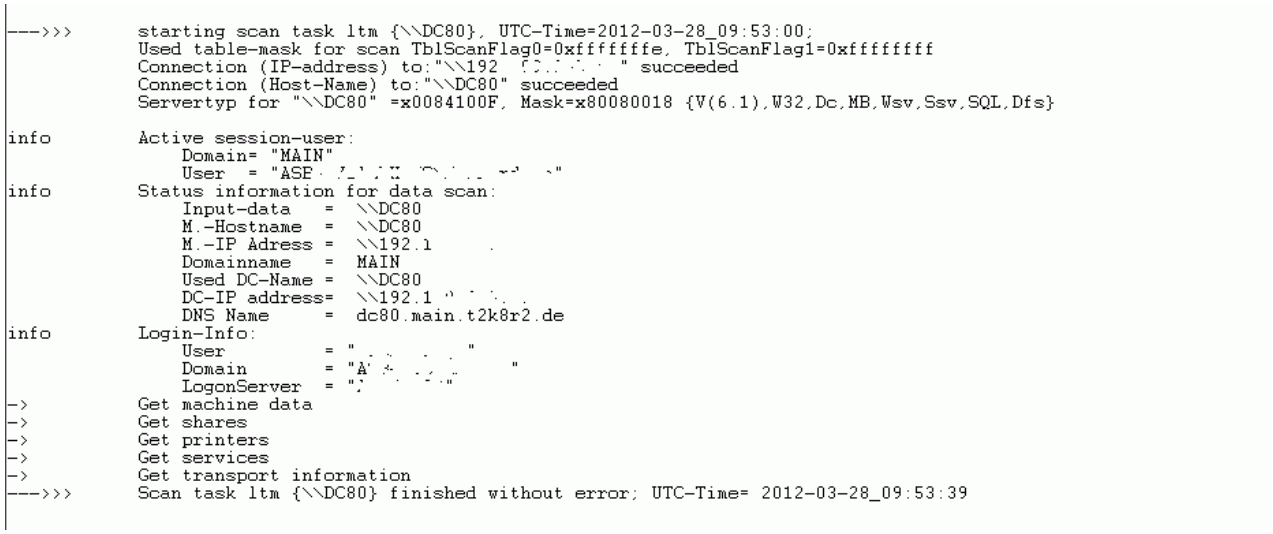


Abbildung 4.25: Administrator Scan Protokoll

Der an den DatenScan sich anschließende Datenimport eines Scan-Jobs wird besonders ausführlich protokolliert:

Ein Import eines Jobs in eine Datenbank erfolgt immer in 2 Teilschritten:

1. Tabellen laden (Loader Process)
2. Tabellen verarbeiten (Qualifier Process: Erstellung der eigentlichen Daten für Ansicht und Reports).

Es besteht die Möglichkeit zusätzliche artfremde Anwendertabellen /Daten zu laden und mit asbLANtools darzustellen.

Protokoll: Import Prozess:

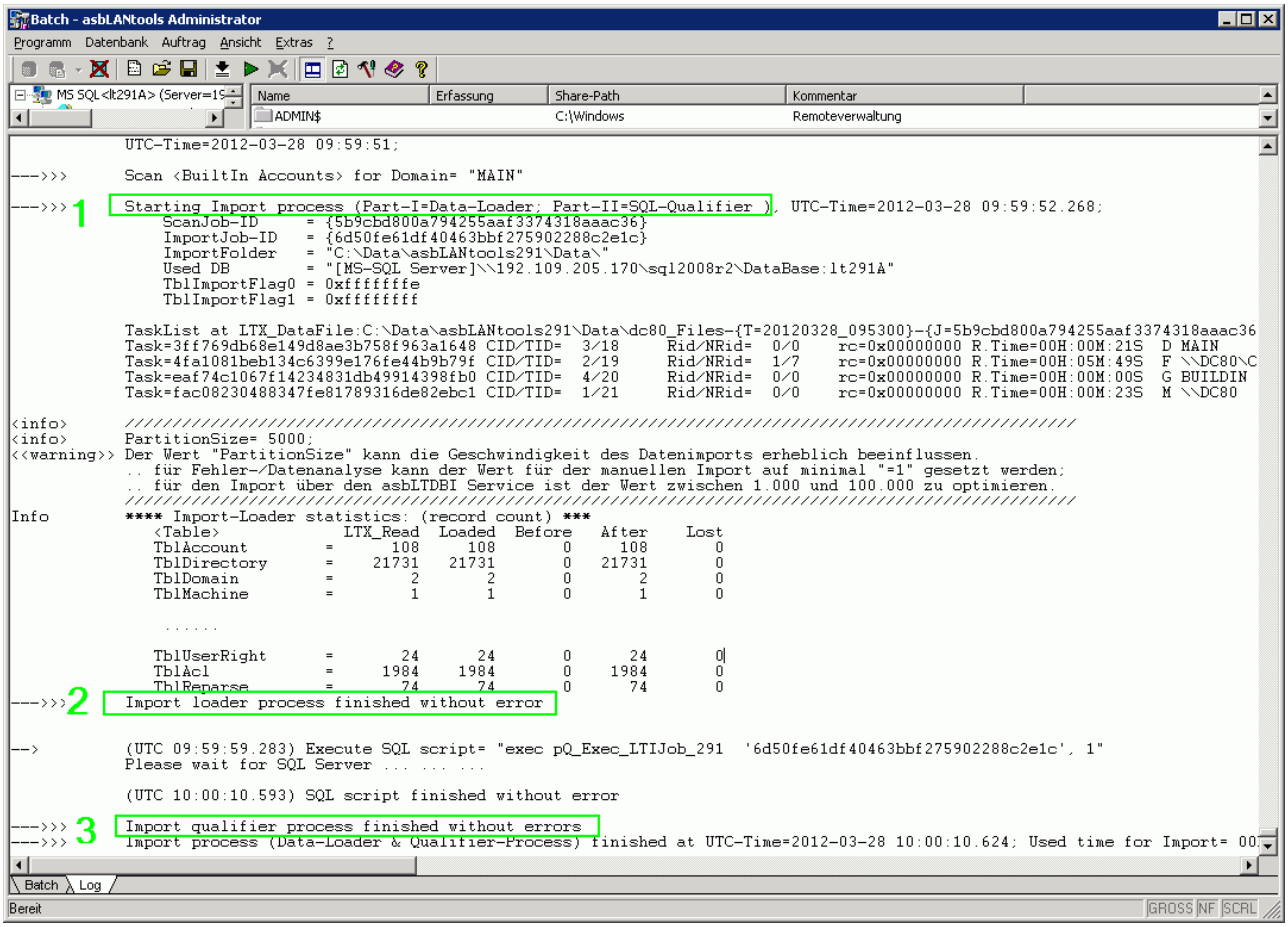

Batch - asbLANtools Administrator
Programm Datenbank Auftrag Ansicht Extras ?
Name Erfassung Share-Path Kommentar
ADMIN$ C:\Windows Remoteverwaltung
UTC-Time=2012-03-28 09:59:51;
Scan <BuiltIn Accounts> for Domain= "MAIN"
1
Starting Import process (Part-I=Data-Loader; Part-II=SQL-Qualifier), UTC-Time=2012-03-28 09:59:52.268;
ScanJob-ID = {5b9cbd800a794255aaf3374318aaac36}
ImportJob-ID = {6d50fe61df40463bbf275902288c2e1c}
ImportFolder = "C:\Data\asbLANtools291\Data\"
Used DB = "[MS-SQL Server]\\192.109.205.170\sql2008r2\DataBase:lt291A"
TblImportFlag0 = 0xfffffffe
TblImportFlag1 = 0xffffffff
TaskList at LTX_DataFile:C:\Data\asbLANtools291\Data\dc80_Files-{T=20120328_095300}-{J=5b9cbd800a794255aaf3374318aaac36
Task=3ff769db68e149d8ae3b758f963a1648 CID/TID= 3/18 Rid/NRid= 0/0 rc=0x00000000 R.Time=00H:00M:21S D MAIN
Task=4fa1081beb134c6399e176fe44b9b79f CID/TID= 2/19 Rid/NRid= 1/7 rc=0x00000000 R.Time=00H:05M:49S F \\DC80\C
Task=eaf74c1067f14234831db49914398fb0 CID/TID= 4/20 Rid/NRid= 0/0 rc=0x00000000 R.Time=00H:00M:00S G BUILDIN
Task=fac08230488347fe81789316de82ebc1 CID/TID= 1/21 Rid/NRid= 0/0 rc=0x00000000 R.Time=00H:00M:23S M \\DC80
<info> //
<info> PartitionSize= 5000;
<<warning>> Der Wert "PartitionSize" kann die Geschwindigkeit des Datenimports erheblich beeinflussen.
.. für Fehler-/Datenanalyse kann der Wert für der manuellen Import auf minimal "=1" gesetzt werden;
.. für den Import über den asbLTDBI Service ist der Wert zwischen 1.000 und 100.000 zu optimieren.
//
Info **** Import-Loader statistics: (record count) ***
<Table> LTX_Read Loaded Before After Lost
TblAccount = 108 108 0 108 0
TblDirectory = 21731 21731 0 21731 0
TblDomain = 2 2 0 2 0
TblMachine = 1 1 0 1 0
.....
TblUserRight = 24 24 0 24 0
TblAcl = 1984 1984 0 1984 0
TblReparse = 74 74 0 74 0
2
Import loader process finished without error
--> (UTC 09:59:59.283) Execute SQL script= "exec pQ_Exec_LTIJob_291 '6d50fe61df40463bbf275902288c2e1c', 1"
Please wait for SQL Server ... ...
(UTC 10:00:10.593) SQL script finished without error
3
Import qualifier process finished without errors
Import process (Data-Loader & Qualifier-Process) finished at UTC-Time=2012-03-28 10:00:10.624; Used time for Import= 00
Batch Log
Bereit
GROSS NF SCRL

Abbildung 4.26: Administrator Import Protokoll

4.5 Modul Viewer

Die Auswertung „erfasster“ Daten bildet den eigentlichen Schwerpunkt der Software asbLAN*tools*. Diesbezüglich wurde der Erfassungsprozess weiter automatisiert um noch leichter und schneller Daten für eine Offline-Auswertung zu erhalten und um mehr Augenmerk auf die Auswertung legen zu können.

Daten zur Auswertung können sowohl direkt aus einem Erfassungsprozess, als auch „archivierten Beständen“ entnommen werden.

Besonders die einfache Möglichkeit jederzeit Daten für eine Auswertung zu importieren, sollte dazu führen, dass die gescannten Daten als „Rohdaten“ auch archiviert werden. Sie auch Kapitel 0 zum Thema Altdatenbestände.

Die Archivierung von kompletten Datenbanken erfordert mehr Zeit und Aufwand und bietet dazu weniger „Bewegungsfreiheit“ für die Auswertung.

asbLANtools Viewer ist die zentrale Komponente zur Auswertung von Daten und die Schnittstelle zur Dokumentation (Reporting).

Zum Start des Moduls Viewer kann dieser über die Gruppe asbLAN*tools* im Menü „Programme“ des Startmenüs oder direkt über Menü „Overview“ geladen werden.

4.5.1 Übersicht

Der asbLANtools Viewer beinhaltet:

- Die Darstellung kompletter Domänen mit Eigenschaften der Benutzer, Gruppen, Maschinen, Dienste Shares, Files und Directorys
- Treeview Darstellung von Verzeichnissen und deren Rechten
- Bottom-Up Technologie zum Aufzeigen von Fehlern oder Änderungen in der Berechtigungsstruktur. Das Aufwendige „Aufklappen“ und Betrachten alle Verzeichnisse, sowie der jeweils darunter liegenden Verzeichnisse entfällt.
- Mehrfach verschachtelte Fehler werden durch einen farbigen Leitfaden dargestellt, „Grün“ (+ „Blau“) ist der Weg zum Fehler.
- Der Viewer bietet die absolut richtige Darstellung der ACL/ ACE Rechtelisten (unter NT4 ein großes Problem, aber auch W2K). Die Rechteliste (Reihenfolge ist wichtig für das „Effektive“ Zugriffsrecht).
- Alle Eigenschaften von Files/ Verzeichnissen werden mit allen NTFS Eigenschaften abgebildet.
- Neben landläufigen Zugriffsrechten werden vor allem „Verbote“ wie sonst nirgends sauber analysiert und dargestellt.
- Auditing- Überwachung von Verzeichnissen und Files werden inklusive Erfolg- und Verbotsüberwachung ausgewertet.
- Der Viewer bietet die Möglichkeit sehr schnell Dateien im Netzwerk durch komplexe Suchroutinen zu finden. Gefundene Dateien können direkt über Befehl „GOTO“ im gesamten Netzwerk selektiert und behandelt werden.
- Eine komplexe Funktion der Rückspeicherung ermöglicht komplette Rechtestrukturen über Verzeichnisbäume wieder herzustellen, sowie alle Gruppen- und Benutzereinträge wieder herzustellen.
- Die ab Windows 2000 komplex verfügbare „Vererbungstechnologie“ ist im Viewer darstellbar (alle Vererbungsbits werden ausgewertet).
  Insbesondere erfolgt eine konsolidierte Darstellung der Vererbung für Objekte, welche aus den einzelnen Vererbungsinformationen der ACE’s zusammengefasst werden.
- Über eine Reportschnittstelle können selektierte Daten gedruckt oder dokumentiert werden.
- Der Viewer beinhaltet ein offenes, flexibles Interface für die Reporterweiterung bzw. Auswertung der Daten mit anderen Tools.
- Die verwendeten Datenbanken sind in Struktur und Technologie auf Leistungsfähigkeit ausgelegt, so dass Netzwerke mit 100.000 Benutzern auswertbar sind.

4.5.2 Datenbank auswählen

Der Viewer arbeitet über eine Datenbank, in welcher alle Daten liegen. Nach dem Starten des Programms erhalten Sie folgende Ansicht:

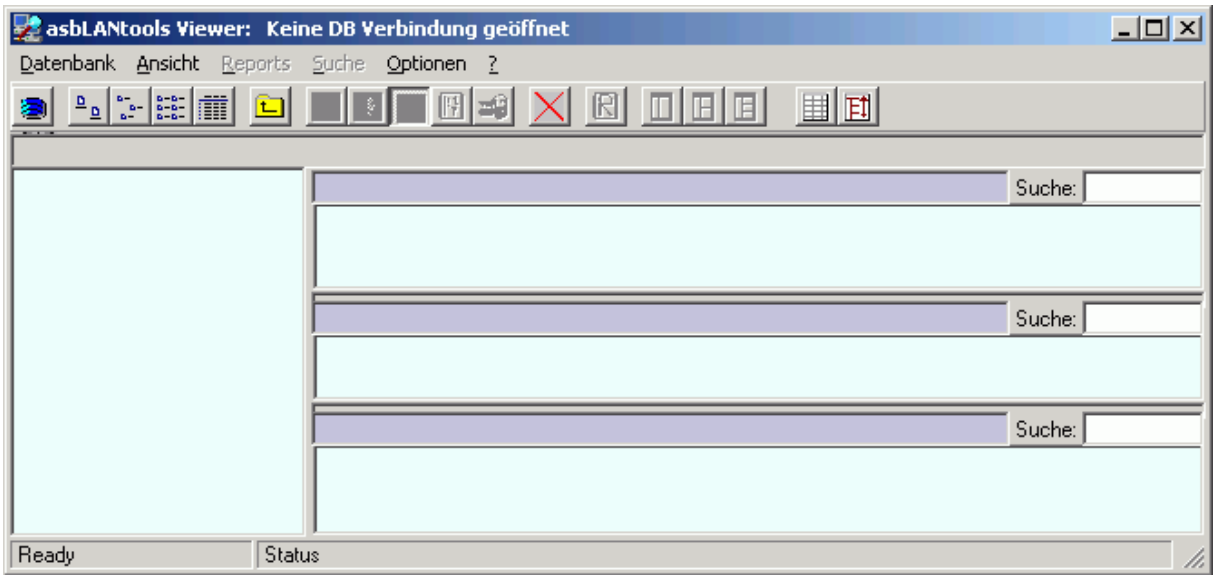


Abbildung 4.27: asbLANtools Viewer Startbildschirm

Im ersten Schritt müssen Sie eine Datenbank-Verbindung öffnen. Der Initial-Bildschirm zeigt 4 Quadranten. Sie können die Bildschirmteilung entsprechend Erfordernis verändern (Art und Anzahl der Fenster). Ferner wird je nach Inhalt einer Darstellung eine geänderte Einstellung durch Steuerung in den „Abfragen“ gewählt.

Durch die Auswahl des Menüs „Datenquelle“ / „Öffnen“ können Sie auf den Datenbank-Anmeldedialog zugreifen und eine Datenquelle vom Typ MS SQL auswählen:

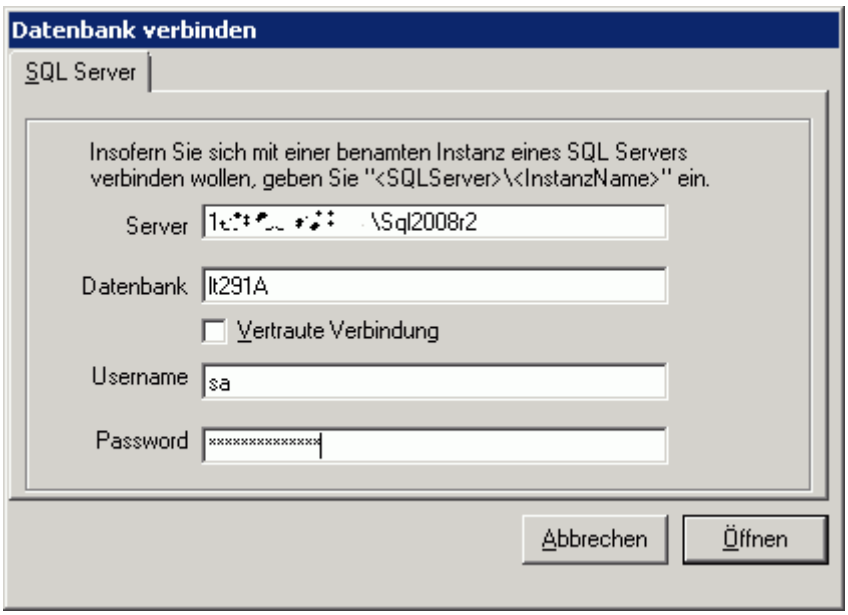


Abbildung 4.28: Die asbLANtools Viewer Datenbankanmeldung

Wählen Sie eine der verfügbaren Datenquellen aus. Die Verbindung zur Datenbank wird „lesend“ hergestellt. Es stehen nun die gespeicherten Informationen für eine Auswertung zur Verfügung.

Zur Nutzung einer Datenbank geben Sie die entsprechenden notwendigen Informationen (siehe Bild) für diese Anmeldung ein.

4.5.3 Bedienoberfläche

Nach Anmeldung an eine Datenquelle werden die Informationen in der Datenbank sichtbar dargestellt. Alle Informationen sind als Treeview(Baumstruktur) organisiert.

Folgende Windows konformen Eingaben sind erlaubt /möglich:

- Eingabe von Kommandos zur Darstellung über die Menüleiste
- Rechte Maustaste zur Darstellung von Detailinformationen selektierter Informationen.
- Selektion von Information kann über Einzel-Selektion (linke Maustaste, Mehrfachselektion „Ctrl-Taste + linke Maustaste; Bereichsselektion = SHIFT + Maustaste Beginn /Ende, sowie Aufspannen eines Fensters mit linker Maustaste) erfolgen. Die Bedienung mit der Maus entspricht Windows-Konformität.

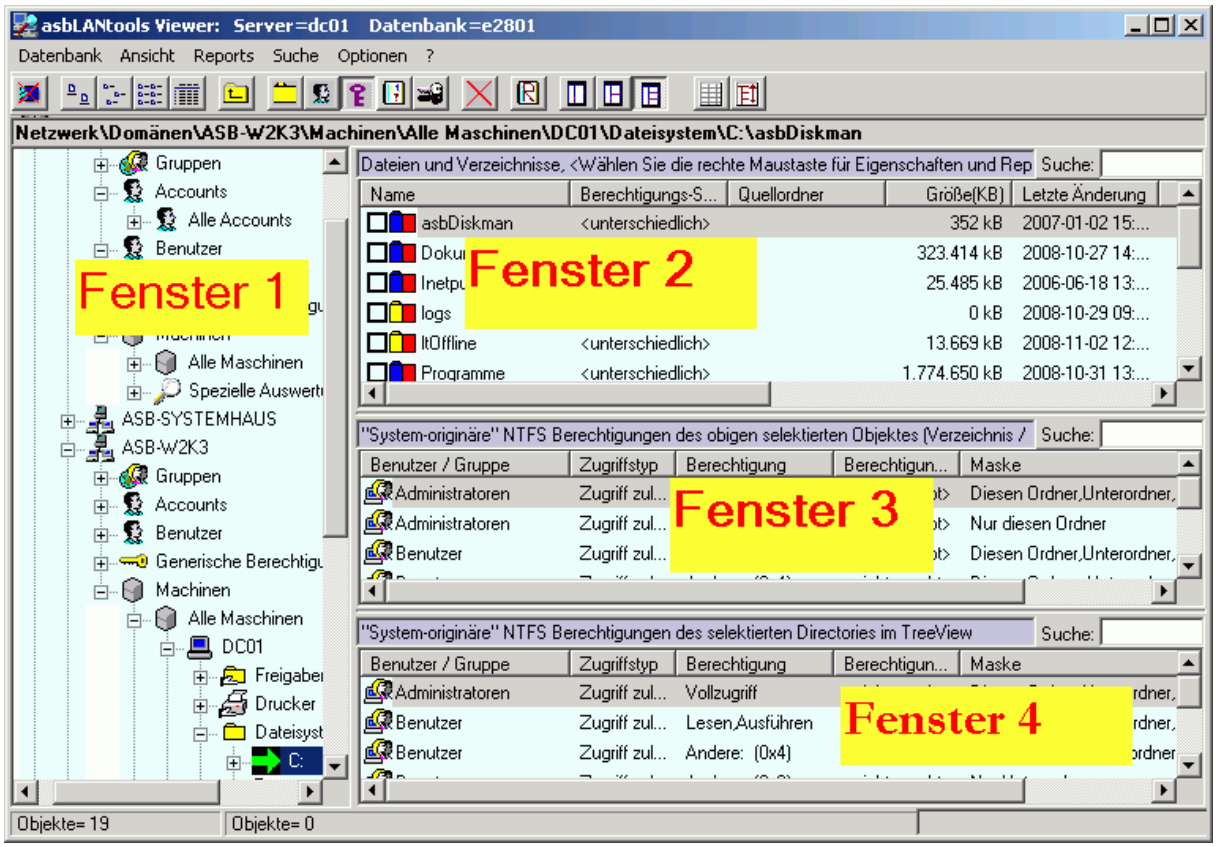


Abbildung 4.29: Der asbLANtools Viewer

Der Bildschirm des asbLAN*tools* Viewer besteht aus bis zu vier separaten Fenstern. Mindestens werden Fenster F1 und F2 angezeigt. In diesen werden die folgenden Informationen angezeigt:

Fenster	Information
F1	Treeview Übersicht der erfassten Objekte in Baumstruktur. Der Baum ist nach Domänen und Maschinen sortiert.

F2	Detailinformationen zu dem im Baum selektierte Objekt. Beispiel: Sind „Konten“ in F1 selektiert wird in F2 die Liste der Benutzer angezeigt, Wird in F1 ein Laufwerk selektiert, werden in F2 die zugehörigen Verzeichnisse angezeigt.
F3	Detailinformationen zu F1: Ist in F1 ein Verzeichnis selektiert, werden in F3 die ACL Listen sichtbar.
F4	Detailinformationen zu F2: analog F3 oder F1 in der Verzeichnisstruktur.

Tabelle 4.2: asbLANtools Viewer, Fensteraufteilung

Generell lässt sich in der aktuellen Version Art, Inhalt und Abhängigkeit der darzustellenden Informationen in den einzelnen Fenstern durch hinterlegte SQL Abfragen steuern. So kann beispielsweise bei Klick auf ein Objekt im Fenster F2 eine Detail-Information im Fenster F3 angezeigt werden während im Fenster F4 die Detailinformation zu F1 selektierten Objekten angezeigt wird. Ferner wird z.B. in Gruppen/Account Darstellungen bei Klick auf ein Objekt in F1 im Fenster F2, F3 und F4 Detailinformationen zum Objekt in F1 dargestellt (Mitglieder einer Gruppe/ abgeleitete Mitglieder, rufende Gruppen).

Die Gestaltung der Menüstrukturen im LTViewer ist nicht Gegenstand dieses Handbuches.

Das Fenster F2 kann in verschiedenen Optionen dargestellt werden:

- Große Symbole
- Kleine Symbole
- Liste, beziehungsweise
- Detailliste

Spezielle Ansichten

In der ausgelieferten Version /Standardansicht befinden sich eine Reihe von Datenansichten, welche Ihnen helfen, sich zu Recht zu finden und im Fall eines Fehlers einen effektiven Support zu erhalten. Damit Sie sich eine Übersicht über Ihre Grundlagen (Arbeitsdaten) machen können, greifen Sie bitte auf die Menüs „Importierte Daten“ zu. Prüfen Sie in einer Kurzform, ob die erforderlichen Aufträge in der Datenbank nach dem Importprozess gespeichert wurden:

Sie können verständlicher Weise nur Daten auswerten, welche auch fehlerfrei in die DB importiert wurden. Prüfen Sie deshalb die importierten Daten:

Sowohl für Domänen, Maschinen als auch Verzeichnisse werden das Scan- und Importdatum ausgewiesen.

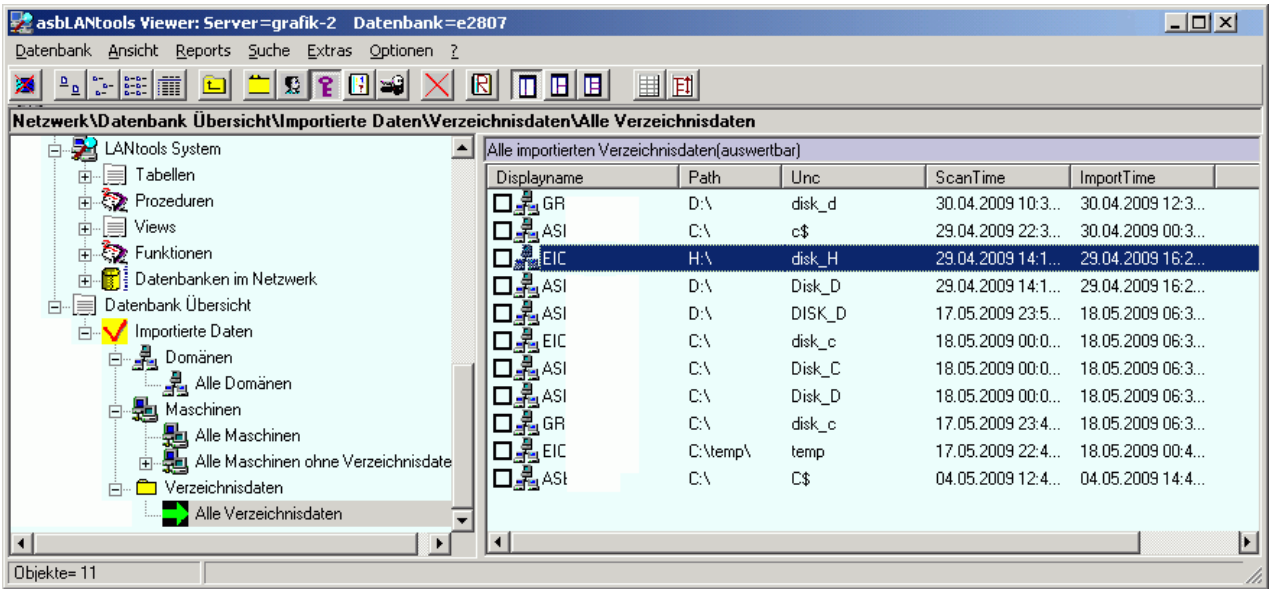

asbLANtools Viewer: Server=grafik-2 Datenbank=e2807
Datenbank Ansicht Reports Suche Extras Optionen ?
Netzwerk\Datenbank Übersicht\Importierte Daten\Verzeichnisdaten\Alle Verzeichnisdaten
LANtools System
Tabellen
Prozeduren
Views
Funktionen
Datenbanken im Netzwerk
Datenbank Übersicht
Importierte Daten
Domänen
Alle Domänen
Maschinen
Alle Maschinen
Alle Maschinen ohne Verzeichnisdate
Verzeichnisdaten
Alle Verzeichnisdaten
Alle importierten Verzeichnisdaten(auswertbar)
Displayname Path Unc ScanTime ImportTime
GR D:\ disk_d 30.04.2009 10:3... 30.04.2009 12:3...
ASI C:\ c$ 29.04.2009 22:3... 30.04.2009 00:3...
EIC H:\ disk_H 29.04.2009 14:1... 29.04.2009 16:2...
ASI D:\ Disk_D 29.04.2009 14:1... 29.04.2009 16:2...
ASI D:\ DISK_D 17.05.2009 23:5... 18.05.2009 06:3...
EIC C:\ disk_c 18.05.2009 00:0... 18.05.2009 06:3...
ASI C:\ Disk_C 18.05.2009 00:0... 18.05.2009 06:3...
ASI C:\ Disk_D 18.05.2009 00:0... 18.05.2009 06:3...
GR C:\ disk_c 17.05.2009 23:4... 18.05.2009 06:3...
EIC C:\temp\ temp 17.05.2009 22:4... 18.05.2009 00:4...
ASI C:\ C$ 04.05.2009 12:4... 04.05.2009 14:4...
Objekte= 11

Abbildung 4.30: Importierte Daten, Datum vom Scan u. Importprozess

Eine besondere Beachtung sollte vor einer Auswertung den dazu zur Verfügung stehenden Daten (Vollständigkeit) gewidmet sein. Dies ist umso bedeutender, insofern es sich um Negativ- oder Vollständigkeitsprüfungen handelt. Dazu besteht die Möglichkeit Tasks und Scans wie nachfolgend dargestellt zu sichten:

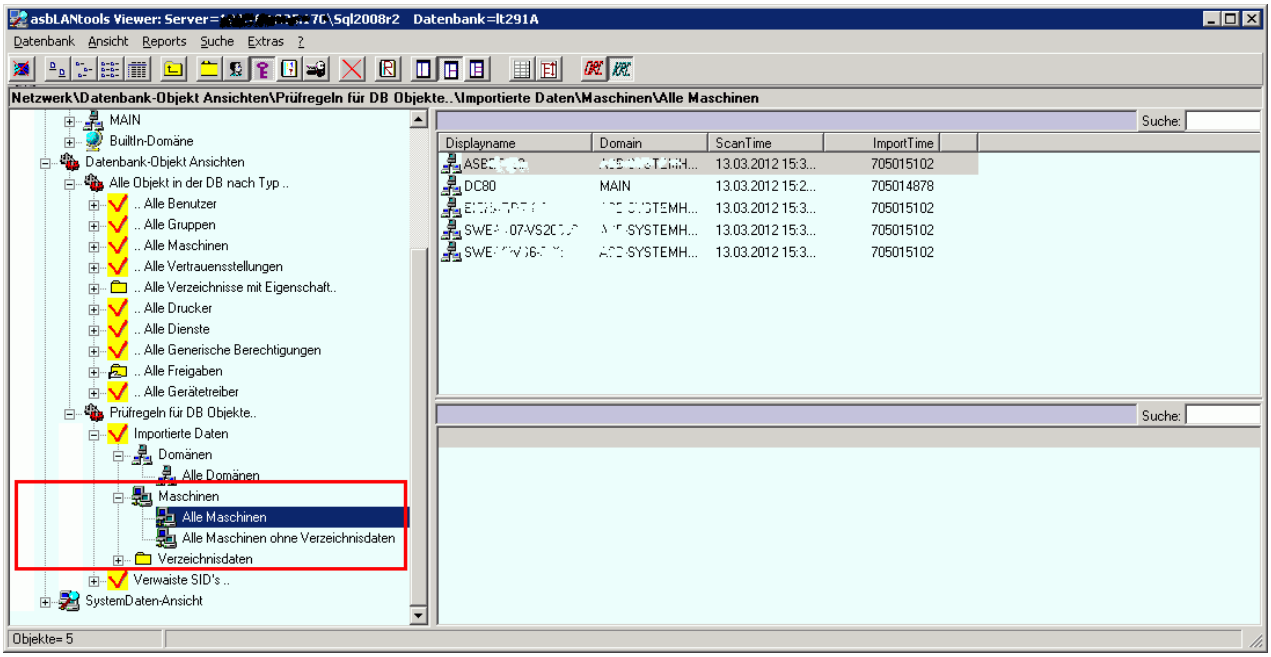


Abbildung 4.31: Prüfregeln für importierte Daten

Es sind Auswertungen wie

- Maschine ohne zugehörige Domäne
- Maschine ohne Filesystem
- Filesystem ohne Maschine
- Alle …

implementiert.

Als Anwender haben Sie die Möglichkeit beliebige Daten zu visualisieren.

Die obige Prüfregel wird dabei in einem oder mehreren, nachfolgend dargestellten SQL Eintrag für den LTViewer Treeview und Listview generiert:

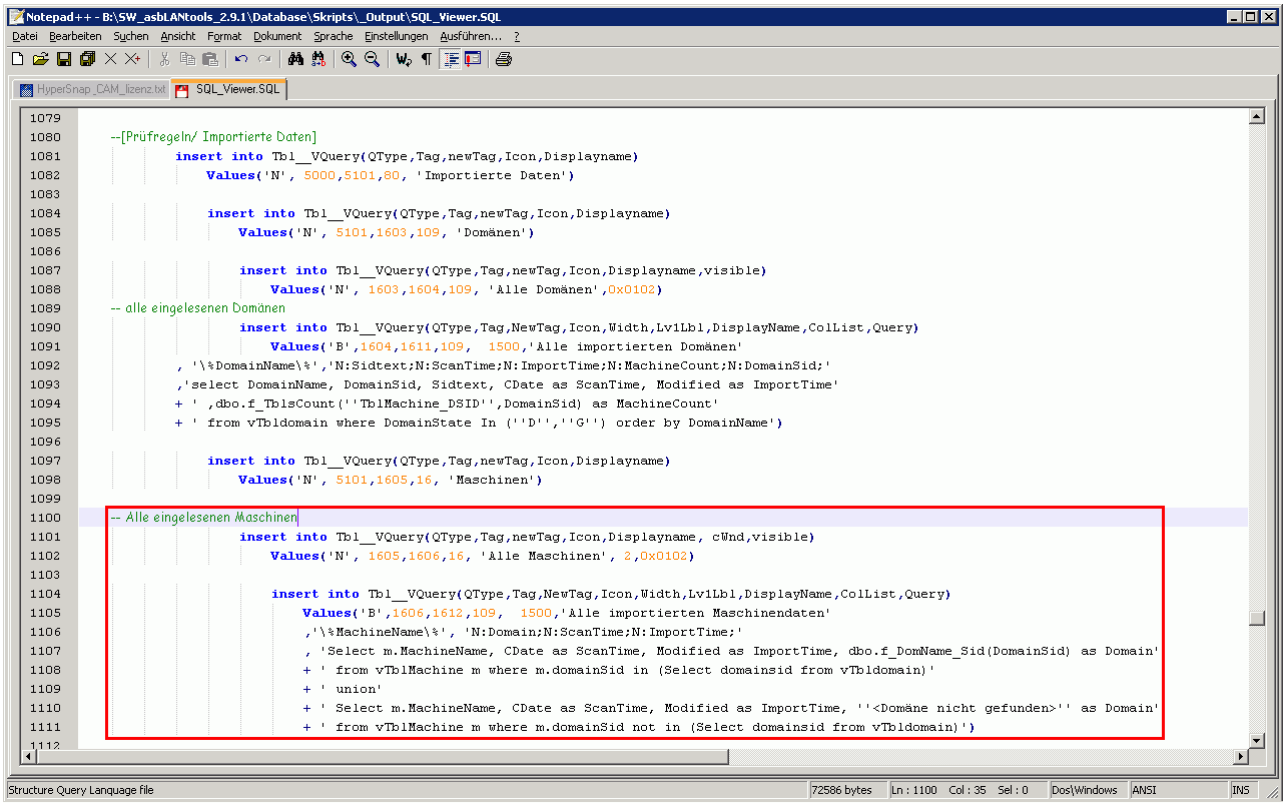

Notepad++ - B:\SW_asbLANtools_2.9.1\Database\Skripts_Output\SQL_Viewer.SQL
Datei Bearbeiten Suchen Ansicht Format Dokument Sprache Einstellungen Ausführen... ?
HyperSnap_CAM_lizenz.txt
SQL_Viewer.SQL
--[Prüfregeln/ Importierte Daten]
insert into Tbl__VQuery(QType,Tag,newTag,Icon,Displayname)
Values('N', 5000,5101,80, 'Importierte Daten')
insert into Tbl__VQuery(QType,Tag,newTag,Icon,Displayname)
Values('N', 5101,1603,109, 'Domänen')
insert into Tbl__VQuery(QType,Tag,newTag,Icon,Displayname,visible)
Values('N', 1603,1604,109, 'Alle Domänen',0x0102)
-- alle eingelesenen Domänen
insert into Tbl__VQuery(QType,Tag,NewTag,Icon,Width,Lv1Lbl,DisplayName,ColList,Query)
Values('B',1604,1611,109, 1500,'Alle importierten Domänen'
, '\%DomainName\%','N:Sidtext;N:ScanTime;N:ImportTime;N:MachineCount;N:DomainSid;'
,'select DomainName, DomainSid, Sidtext, CDate as ScanTime, Modified as ImportTime'
+ ' ,dbo.f_TblsCount(''TblMachine_DSID'',DomainSid) as MachineCount'
+ ' from vTbldomain where DomainState In (''D'',''G'') order by DomainName')
insert into Tbl__VQuery(QType,Tag,newTag,Icon,Displayname)
Values('N', 5101,1605,16, 'Maschinen')
-- Alle eingelesenen Maschinen
insert into Tbl__VQuery(QType,Tag,newTag,Icon,Displayname, cWnd,visible)
Values('N', 1605,1606,16, 'Alle Maschinen', 2,0x0102)
insert into Tbl__VQuery(QType,Tag,NewTag,Icon,Width,Lv1Lbl,DisplayName,ColList,Query)
Values('B',1606,1612,109, 1500,'Alle importierten Maschinendaten'
,'\%MachineName\%', 'N:Domain;N:ScanTime;N:ImportTime;'
, 'Select m.MachineName, CDate as ScanTime, Modified as ImportTime, dbo.f_DomName_Sid(DomainSid) as Domain'
+ ' from vTblMachine m where m.domainSid in (Select domainsid from vTbldomain)'
+ ' union'
+ ' Select m.MachineName, CDate as ScanTime, Modified as ImportTime, ''<Domäne nicht gefunden>'' as Domain'
+ ' from vTblMachine m where m.domainSid not in (Select domainsid from vTbldomain)')
Structure Query Language file
72586 bytes
Ln : 1100 Col : 35 Sel : 0
Dos\Windows
ANSI
INS

Abbildung 4.32: LTViewers: Auszug aus der Konfiguration

Die Nutzung und Anpassung der Konfiguration des LTViewers bedarf guter SQL Kenntnisse.

Große Datenmengen visualisieren

Bei der Auswahl eines Objektes im Treeview werden alle abhängigen Informationen aus dem Datenbankserver durch eine oder mehrere Abfragen ermittelt und in den Listenfenstern dargestellt. Bei großen Datenmengen, oder „überlasteten“ Servern kann es zu Verzögerungen im Bildaufbau kommen.
In der aktuellen Version kann der Bildaufbau jederzeit durch **<ESC> Taste** oder in der Ikonenleiste enthaltenen Button Abbruch unterbrochen werden:

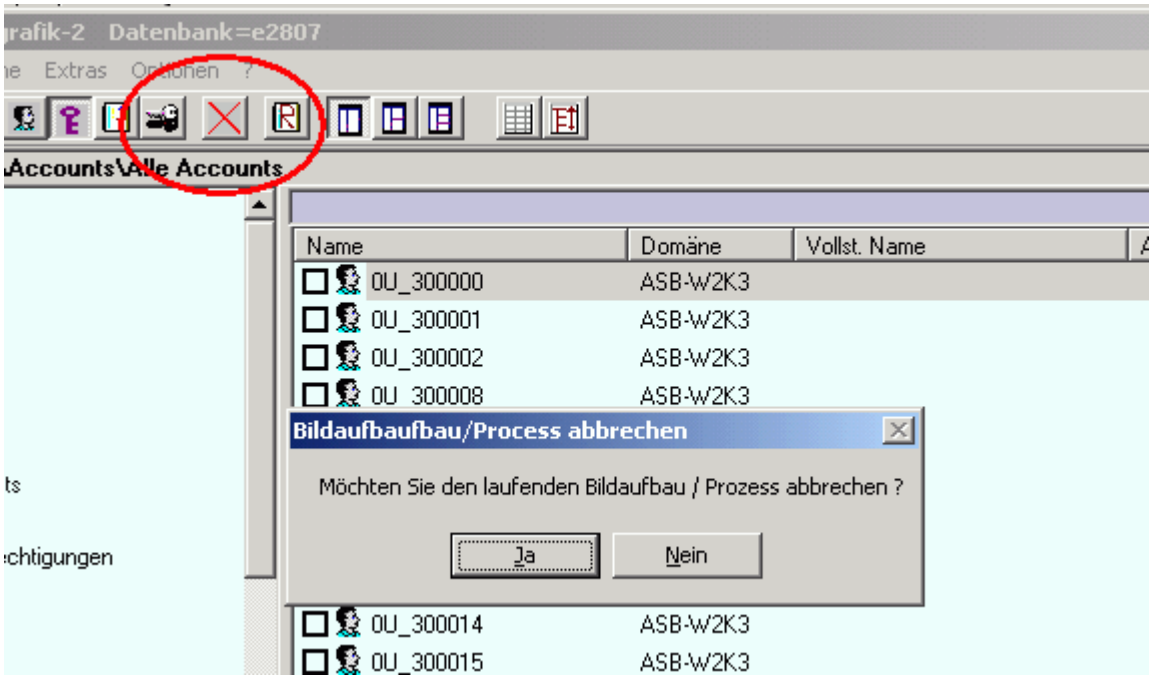


Abbildung 4.33: Bildaufbau unterbrechen

4.5.4 Informationen suchen

Um gezielte Informationen im LTViewer zu suchen stehen verschiedene Möglichkeiten zur Verfügung:

- Sortierung nach einzelnen Spalten
  In der Listenansicht können Sie nach allen Spalteninhalten sortieren. Dabei werden die Inhalte entsprechend Datentyp sensitiv sortiert (Text/Zahl/Datum).
- Die Listenansichten enthalten in der Kopfzeile eine Schnellansicht
  Die Schnellansicht bietet die Möglichkeit über in der Display-Spalte dargestellte Informationen ein Objekt zu selektieren.
- Suche über Suchmenüs (Menü Suche)
  Die Sucher erfolgt immer über die in der Datenbank enthaltenen Daten.
- Filterfunktionen (über Markierungs-Symbol in der Listenansicht)
  => noch nicht freigeschaltet;
  Die Filterfunktion biete die Möglichkeit in einer Ansicht enthaltenen Daten nur gezielte Informationen anzuzeigen und darzustellen. Über Menü „Ansicht Alle/ nur markierte /nicht markierte“, bzw. Menü „Auswahl Selektion zur Markierung zufügen /von Markierung löschen“ stehen effektive Möglichkeiten zur „Mengenoperation“ bereit.

Menü Dateisuche

Durch Auswahl des Befehls „Suchen“ im Menü „Extras“ können Sie Objekte sehr schnell in der Datenbank finden. Vor allem in einer Datenbank größeren Inhaltes kann das Suchen von Informationen vorteilhaft sein.

Über eine Menüauswahl können verschiedene Suchfunktionen für Objekte innerhalb der Datenbank ausgewählt werden:

Register	Bedeutung

Maschine	Hier können Sie nach Maschinen suchen.
Freigaben	Über diese Option können Sie nach Freigaben auf einem der erfassten Server suchen.
Verzeichnisse	Sie können in diesem Register nach Verzeichnissen suchen.
Dateien	Dieses Register müssen Sie auswählen, um nach Dateien zu suchen.
Konto	Sie können als Suchbegriff einen Benutzer- oder Gruppennamen angeben und nach diesem suchen.

Tabelle 4.3: Suchfunktionen im LTViewer

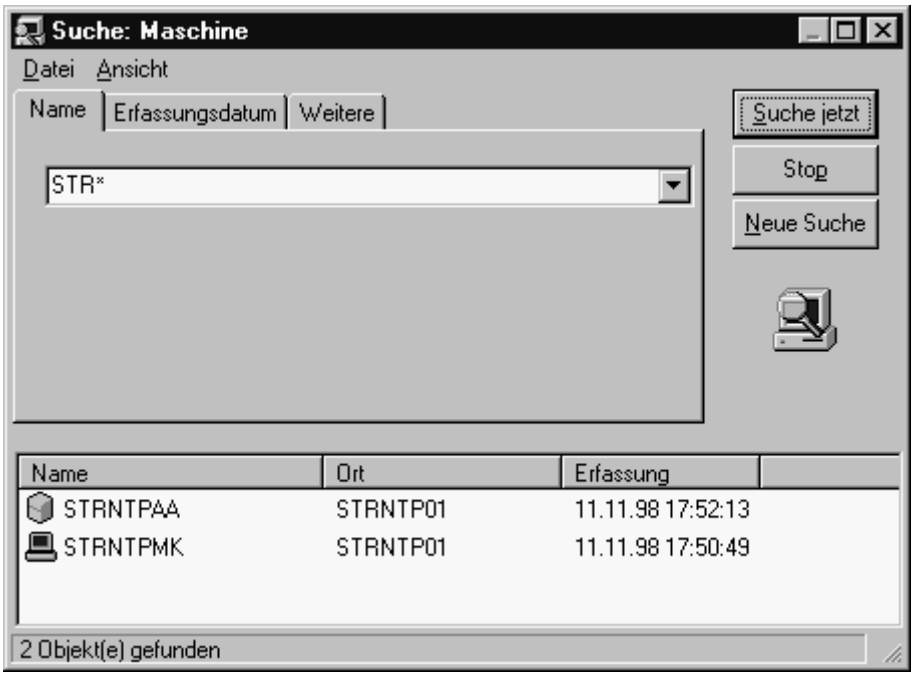


Abbildung 4.34: Die Suchfunktion des asbLANtools Viewer für Maschinen

Der Suchdialog ist objekt-selektiv gestaltet. Weitere Einschränkungen können vorgenommen werden.

Die Suche von Dateien und Verzeichnissen über asbLANtools ist eine sehr leistungsfähige (schnelle) und effektive Methode.

Die im Suchfenster gefundenen Objekte (Files und Verzeichnisse, Shares) können sodann über ein Kontextmenü unter Zuhilfenahme des Microsoft Explorers in der gesamten Domäne ausgewählt selektiert werden.

Die Eingabe von Wildcards „*“ sind in der Suchmaske /Eingabe zulässig.

4.5.5 Kontext sensitive Menüs

Über Kontext sensitive Menüs können im Fenster F2 über die rechte Maustaste unterschiedliche (vom Objekt-Typ abhängige Auswahlmenüs) genutzt werden:

- Menü Eigenschaft
- Menü Report
  steuert den Aufruf zu einem verfügbaren Report. Sie müssen dazu gegebenenfalls

über „Drucker“ / „Einstellungen“ im Menü „Datei“ den Standard-Drucker festlegen und konfigurieren.

- Menü Skriptgenerierung
  ermöglicht die Ausgabe von Batch-Dateien mit Anweisungen zur Generierung /Anlegen dieser auf einem System. Benutzung der Skriptsteuerung siehe Datenausgabe /Skriptsteuerung.
  Damit können Benutzer, Gruppen und Berechtigungen
  - zu einem späteren Zeitpunkt wiederhergestellt werden
  - auf ein anderes System übertragen werden
  - sehr einfach „Kopien“ für Testumgebungen generiert werden
    sowie andere Aufgaben erledigt werden.

4.5.6 Eigenschaftsfenster

Zu allen Objekt-Typen existieren Anzeigen mittels Eigenschaftsfenstern. Diese werden mittels rechter Maustaste im Fenster F2 gewählt.

Die Anzeige der Eigenschaftsfenster unterscheidet sich in Abhängigkeit vom ausgewählten Objekt.

Für Dateien und Verzeichnissen werden die folgenden Eigenschaftsregister dargestellt:

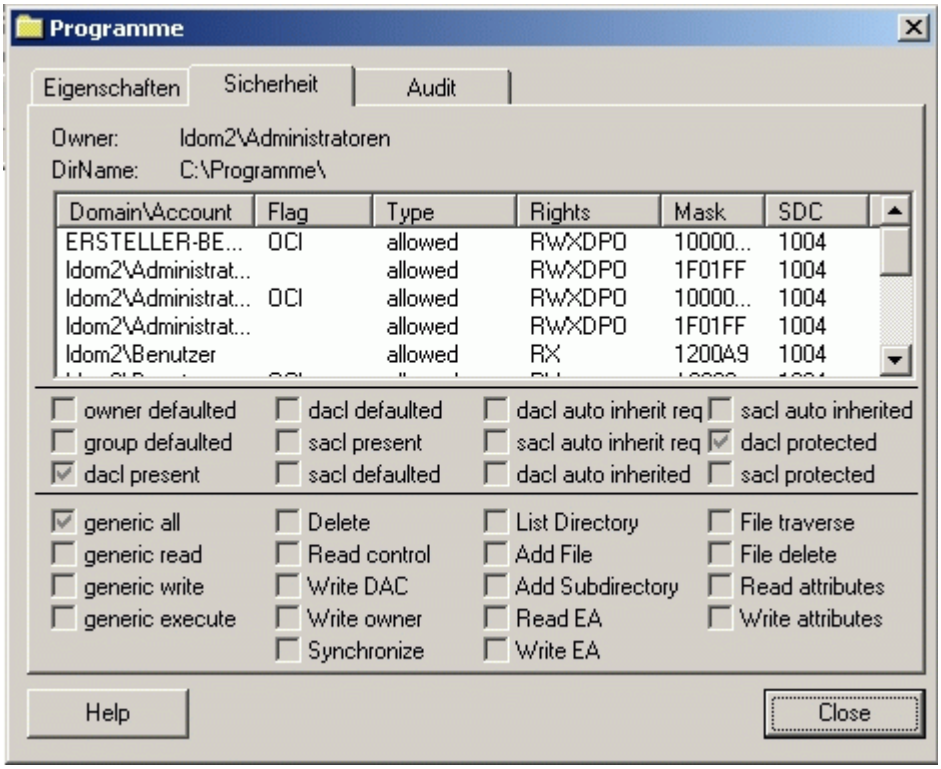


Abbildung 4.37: Eigenschaftsfenster Zugriffsrechte für Dateien/ Verzeichnis

Die ACL-Register (DACL =Zugriffsrechten und SACL = Überwachung von Zugriffen) werden in der systemgenauen „Eintragungsreihenfolge“ des NTFS Dateisystems dargestellt. Dies ist wichtig für die spezifischen Zugriffsrechte und Auswertungen. Sowohl im MS Explorer (verschiedene Ausgaben) als auch anderen Tools wird dies immer wieder vernachlässigt). Bedeutung der Security-Flags für File-/Verzeichnisobjekte:

I	Inherit Only	Vererbungsflag
O	Objects	Recht wird nur auf Dateien vererbt.
C	Container	Recht wird nur auf Verzeichnisse vererbt.

Die Anzeige von Rechte in der Notation RWXDPO ist eine Kurzfassung der Bitmaske der Zugriffsmaske. Es kann in der Praxis eine Vielzahl von Kombinationen von 18 Bits auftreten. Nicht immer ist eine eindeutige Notation RWXDPO darstellbar.

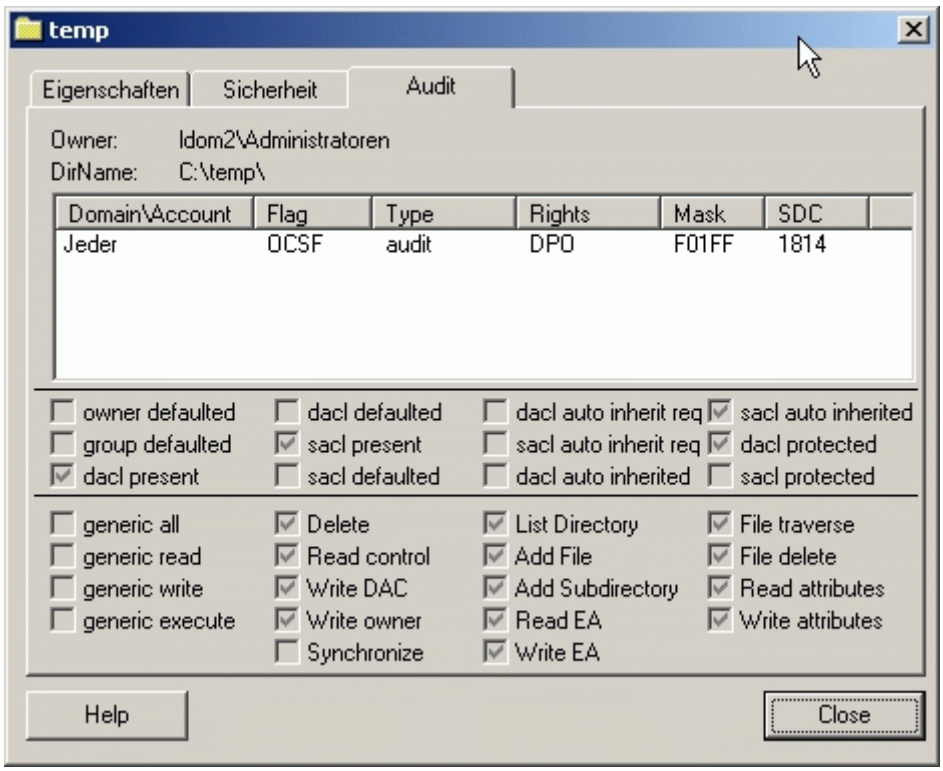


Abbildung 4.38: Eigenschaftsfenster Audit-Rechte für Dateien und Verzeichnisse

Zusätzlich zur DACL Liste werden in der SACL Liste folgenden Flags verwendet:

S	Security	Überwachung von erfolgreichen Zugriffen
F	Failure	Überwachung von fehlerhaften Zugriffen.

In dem obigen Beispiel werden „D“, „P“ und „O“ Zugriffe im Verzeichnis C:\TEMP im Erfolgs- und Fehlerfall überwacht. Die Überwachung wird auf neue Objekte „C“ (Container) und „O“ (Files) übertragen. Weiterhin wird die „Überwachung“ vererbt (nicht kopiert) und die Zugriffsrechte werden nicht vom „Elternobjekt „C:\“ vererbt (DACL_Protected).

Die in asbLANtools integrierte Report- (Druck-)Funktion wird über den Modul Viewer aufgerufen.

Beim Aufruf von der Reportfunktion werden 2 Optionen unterschieden:

Globale Reports (Netzwerk-Report „N“). Diese Reports werten alle verfügbaren Daten in einer DB aus.

Sensitive Reports (über Vorauswahl von Single-/Multiobjekten) über die rechte Maustaste zu aktivieren (siehe Kapitel 4.5.3.).

4.5.7 Analysefunktionen im Detail

Nachdem im letzten Abschnitt ein Überblick über die Analysefunktionen der asbLAN*tools* gegeben wurde, werden in den folgenden Abschnitten die Informationen für die verschiedenen gesammelten Informationen noch detaillierter betrachtet.

Benutzerinformationen

Benutzerkonten werden entsprechend der Windows Philosophie erfasst und dargestellt. Somit werden die Konten in dem jeweiligen Teilbaum der Domäne und die lokalen Konten im Teilbaum der zugehörigen Maschine angezeigt. Für alle Informationen und Konten besteht in dem Datenbankmodell eine relationale Beziehung auf Basis der System-Identifikatoren (SID). Informationen können so eindeutig abgebildet und während der „Lebensdauer“ eines Identifikators auch verfolgt werden.

Benutzerkonten und Gruppen die umbenannt werden sind immer noch eineindeutig zuordenbar. Ebenso können gelöschte und „wiederhergestellte“ Konten voneinander unterschieden werden. Dies ist ein großer Vorteil von asbLANtools.

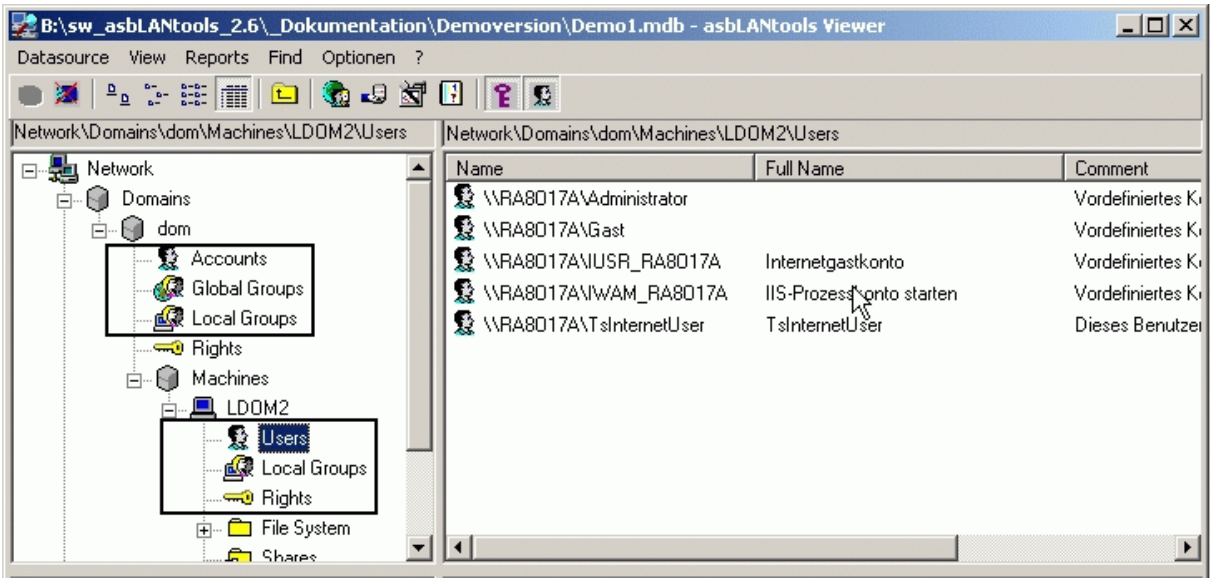


Abbildung 4.39: Die Benutzerkonten

Die Eigenschaften einzelner Konten können visuell am Bildschirm über Kontextmenü gesichtet oder über Druckmenü (Mehrfachauswahl) gedruckt werden.

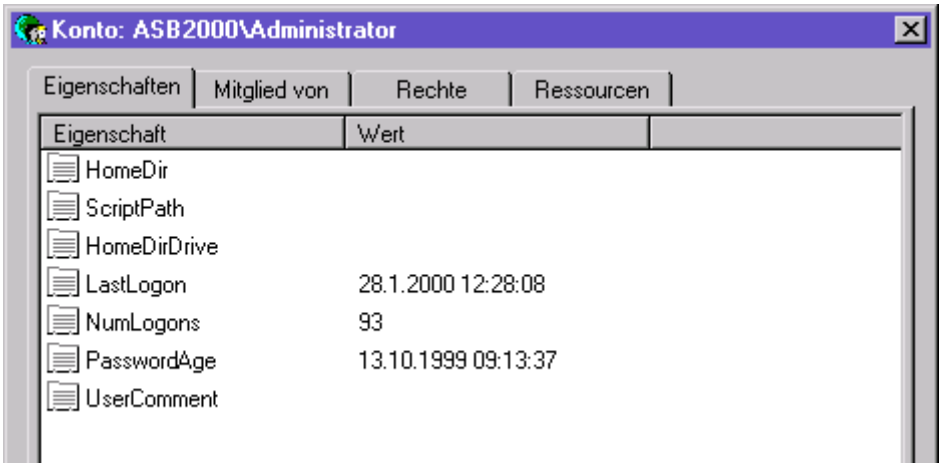


Abbildung 4.40: Dialog Eigenschaften eines Benutzer

Im Register „Eigenschaften“ finden Sie allgemeine Informationen über den Benutzer wie den vollständigen Namen, die Informationen zum Benutzerprofil, zum letzten Anmeldedatum am PDC, der Zahl der Anmeldungen und zum Datum, an dem das Kennwort definiert wurde.

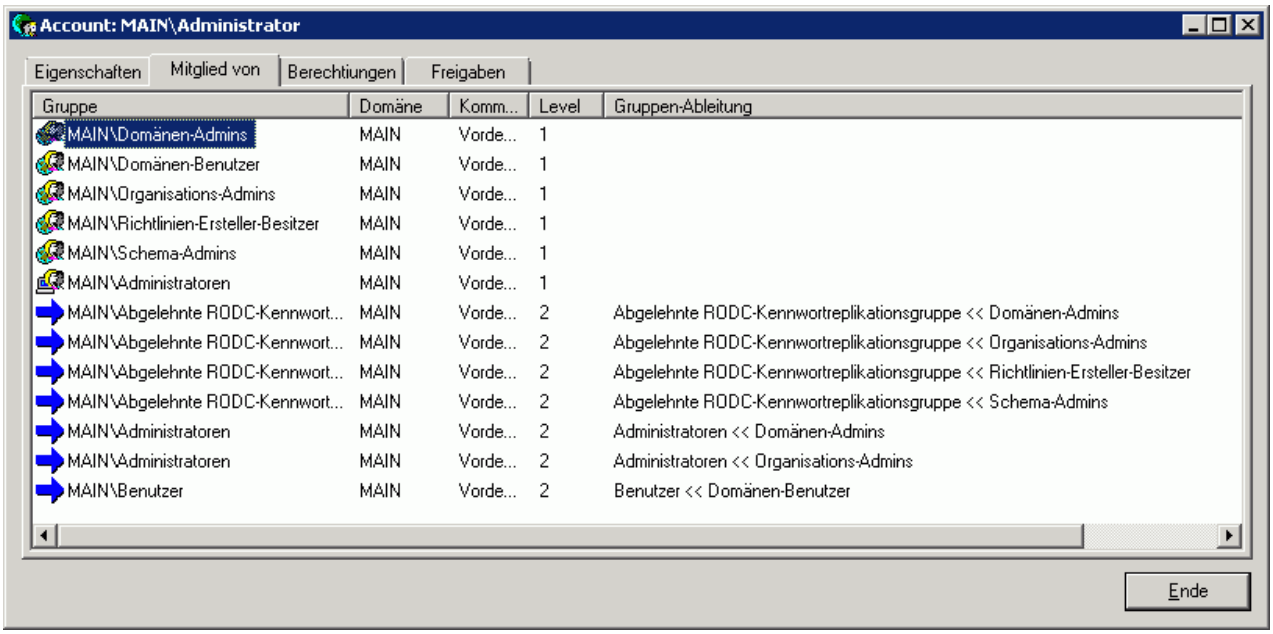


Abbildung 4.41: Dialog Benutzer ist Mitglied von Gruppe XY

Im Register „Mitglied von“ werden die Gruppenzugehörigkeiten für diesen Benutzer angezeigt. Hier werden sowohl die Zuordnungen zu lokalen als auch zu globalen Gruppen in einer Liste zusammengefasst.

Globale Gruppen sind am Symbol mit der Weltkugel und lokale Gruppen am Symbol mit dem Computer erkennbar.

Ferner werden im unteren Teil die abgeleiteten Mitgliedschaften gelistet.

Abbildung 4.42: Dialog Rechte für einen Benutzer

Im Register „Rechte“ werden die Benutzerrechte im Betriebssystem, die dem Benutzer direkt zugeordnet sind, angezeigt. Dieses Register ist bei den meisten Benutzern leer, da solche Rechte in der Regel über Gruppen und nicht direkt an Benutzer vergeben werden.

Abbildung 4.43: Dialog Ressourcen für einen Benutzer

Im Register „Ressourcen“ wird eine Liste der Freigaben (Ressourcen) angezeigt, bei denen der Benutzer Zugriffsrechte besitzt. Auch dieses Register ist in den meisten Fällen leer, da Freigaben in der Regel auf Gruppen- und nicht auf Benutzerebene zugeordnet werden.

Durch Auswahl eines Benutzers können Sie im unteren rechten Fenster eine Liste der zugeordneten Ressourcen mit den Zugriffsrechten anzeigen lassen.

Begriffsdefinition lokale und globale Gruppen

Als lokale Gruppen werden alle Maschinen lokalen Gruppen gekennzeichnet.
Alle anderen Gruppen, welche wiederum selbst Mitglied einer anderen Gruppe sein können, werden als globale Gruppe geführt.

Die Unterscheidungsmerkmale Maschinen-lokal/ Domänen-lokal/ Domänen-global/ Universal /Security Group sind in den erweiterten Eigenschaften gespeichert. Sie haben jedoch auf die „Sicherheitsauswertung eben nur dann eine Auswirkung, wenn Sie den Objekten zugeordnet werden können. Zur vereinfachten Darstellung wird die Unterscheidung lokale /globale Gruppe in asbLANtools weitestgehend beibehalten so wie Sie von MS als „ NTLM Basis –Type auch im AD verwendet wird. Vollständige Attribute finden Sie auch in den Ergebnissen eine AD Scans.

Eine im LTViewer derzeit implementierte Gruppen-Spezifikation sieht wie folgt aus (Anpassung und Änderung sind möglich):

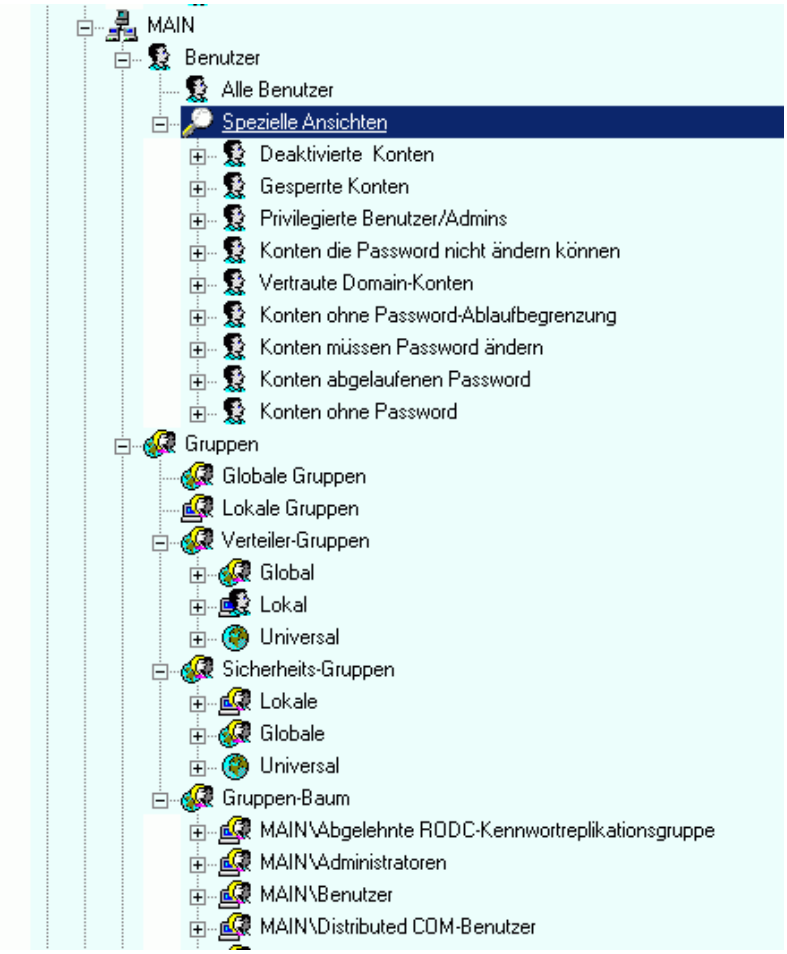


Abbildung 4.44: Gruppendarstellung

Globale Gruppen

Die Informationen, die zu den globalen Gruppen angezeigt werden können, entsprechen weitgehend denen, die auch zu Benutzern angezeigt werden können. Daher wird nachfolgend nur auf die Unterschiede eingegangen.

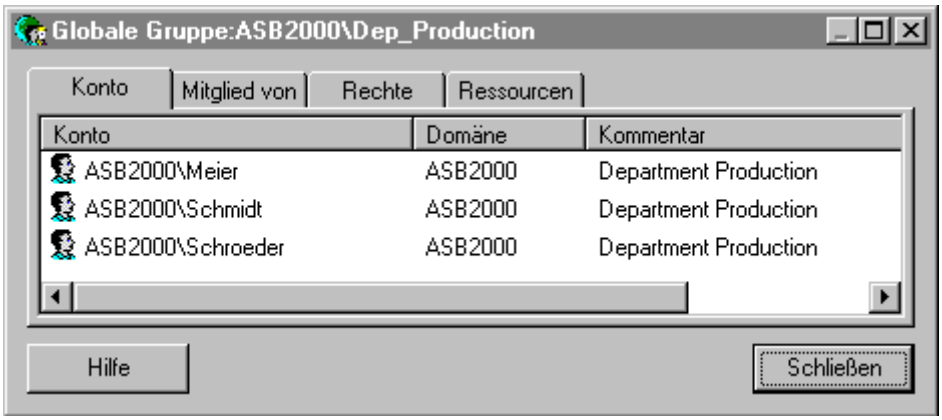


Abbildung 4.45: Das Register Konto für eine globale Gruppe

Der wichtigste Unterschied liegt beim Register „Konto“. Hier wird eine Liste der Benutzer, die der ausgewählten Gruppe zugeordnet sind, ausgegeben.

Die weiteren Register unterscheiden sich nur graduell. Im Register „Mitglied von“ werden bei globalen Gruppen lokale Gruppen angezeigt, in denen der

jeweilige Benutzer Mitglied ist. Bei dem Register „Rechte“ werden Benutzerrechte angezeigt, die der Gruppe zugeordnet wurden und bei dem Register „Ressourcen“ werden alle der Gruppe zugeordneten Rechte auf Netzwerkfreigaben dargestellt. Auch hier gilt, dass bei globalen Gruppen oft nichts angezeigt wird, wenn Benutzerrechte und Freigaben den lokalen Gruppen zugeordnet werden.

Lokale Gruppen

Bei den lokalen Gruppen gibt es nur geringe Unterschiede zu den Eigenschaften der globalen Gruppen. Hier sind vor allem die folgenden Punkte zu beachten:

Lokale Gruppen haben in den meisten Fällen nur globale Gruppen als Mitglieder.

Benutzerrechte und Freigaben (Ressourcen) werden in aller Regel den lokalen Gruppen zugeordnet. Es gilt auch hier, dass durch Auswahl einer lokalen Gruppe im oberen rechten Fenster im unteren rechten Fenster eine Liste der Freigaben angezeigt wird, auf die diese Gruppe Zugriffsrechte besitzt.

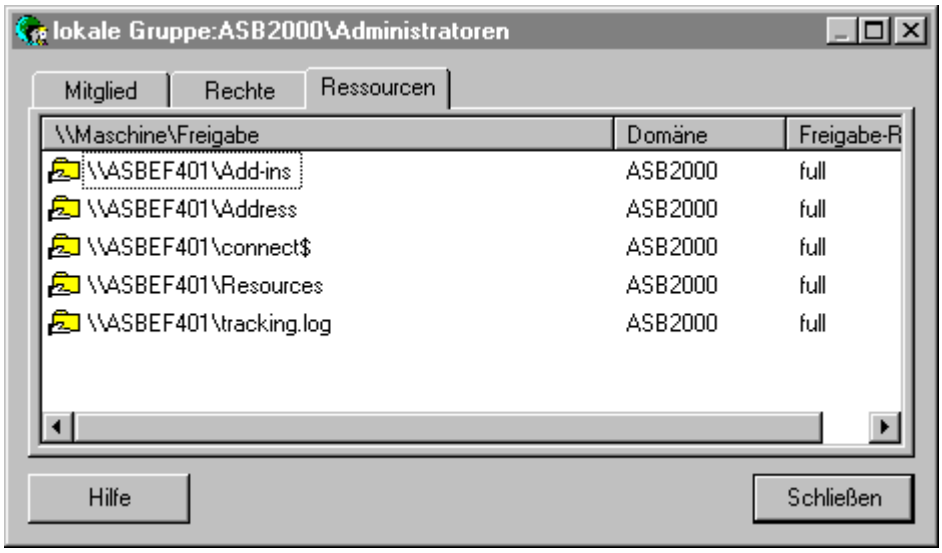


Abbildung 4.46: Freigaben über lokale Gruppen

Benutzerrechte

Wenn Sie im linken oberen Fenster den Zweig „Rechte“ auswählen, werden rechts alle Benutzerrechte des Betriebssystems angezeigt. Sie können in dieser Liste ein Recht auswählen, um im unteren rechten Fenster die Benutzer oder Benutzergruppen angezeigt zu bekommen, denen dieses Recht zugeordnet wurde.

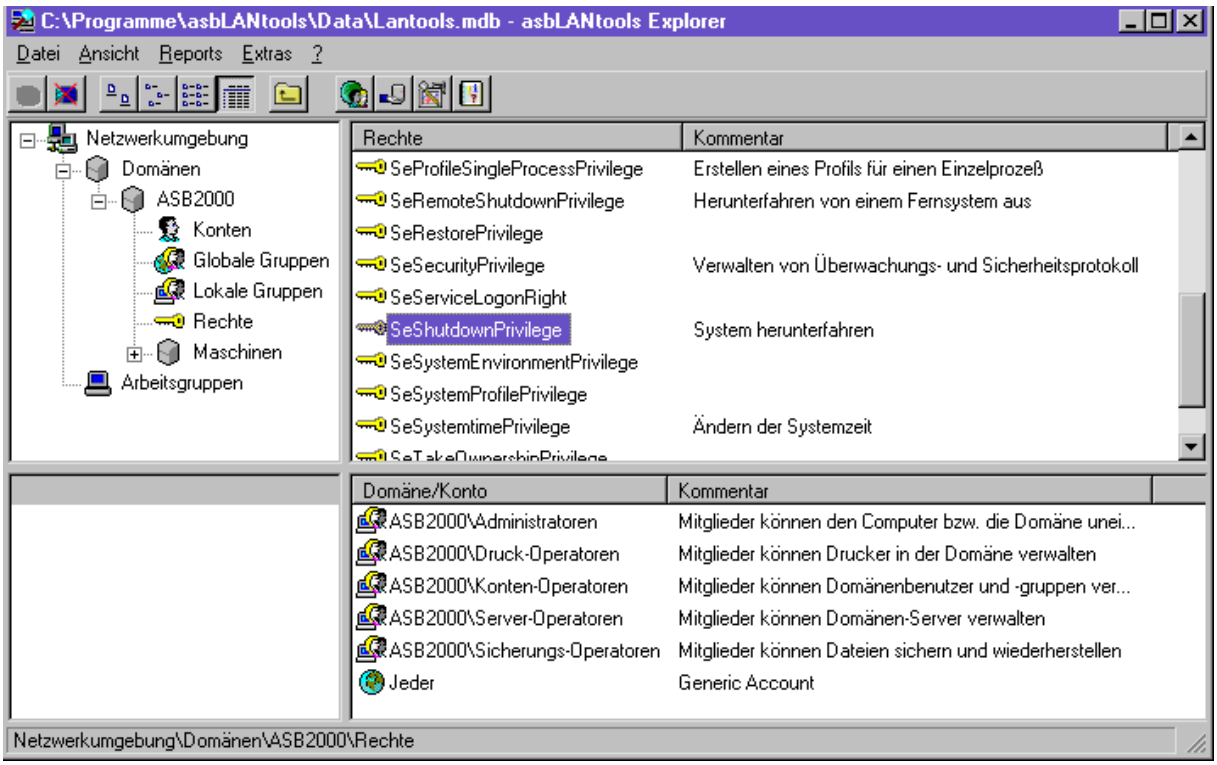


Abbildung 4.47: Die Benutzerrechte und zugeordnete Gruppen

Maschinen

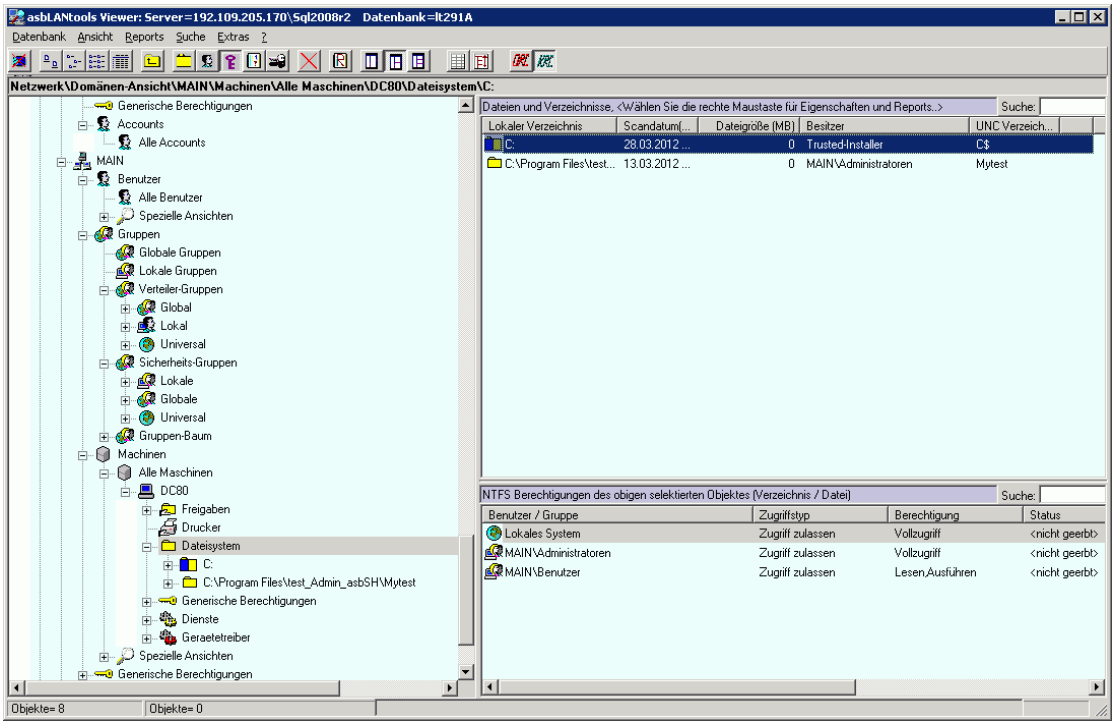


Abbildung 4.48: Der asbLANtools Viewer, erfasste Dateisysteme

Sehr umfangreiche Informationen über die Zugriffsrechte im System können Sie sich unterhalb des Bereichs Maschinen im linken oberen Fenster ausgeben lassen.

Bei Auswahl von Dateisystem unterhalb einer Maschine sehen Sie im rechten oberen Fenster zusammenfassende Informationen über diesen Bereich. Dabei sind immer nur

die Informationen über die von den asbLAN*tools* eingesammelten Bereiche des Dateisystems verfügbar.

Durch einen Doppelklick auf Dateisystem oder Auswahl des Pluszeichens davor können Sie den Bereich expandieren und eine Liste der erfassten Dateisysteme auf der ausgewählten Maschine anzeigen lassen. Sie können so die Dateisysteme systematisch durchblättern.

4.5.8 Auswertung Filesystem /Verzeichnisbäume

Die ab Version 2.8 eingesetzte offene Technologie des LTViewer ermöglicht eine variable Gestaltung der darzustellenden Informationen.
Dazu gehört auch die Darstellung „komprimierter Informationen“ in hierarchischen Strukturen (Verzeichnisbaum mit NTFS Struktur).
Eine effektive und visuelle aussagekräftige Darstellung von Berechtigungen im Filesystem ist eine der starken Eigenschaften von asbLANtools. Derzeit werden Filesysteme nur über die bekannten Standard-Baumstrukturen Domäne/Maschine/Disk-Root/ visualisiert. Es können mit asbLANtools Viewer aber auch Ansichten über alle „Verzeichnisbaume“, oder speziell, durch eine SQL Abfrage gestaltete Abfragen visualisiert werden. Beispiel: Visualisierung aller SQL Server Datenverzeichnisse für effizientere Kontrolle in einem großen Unternehmen mit vielen SQL Daten-Servern. Der DB Administrator erhält nur den notwendigen visuellen Zugriff auf die Ihn interessierenden Daten.

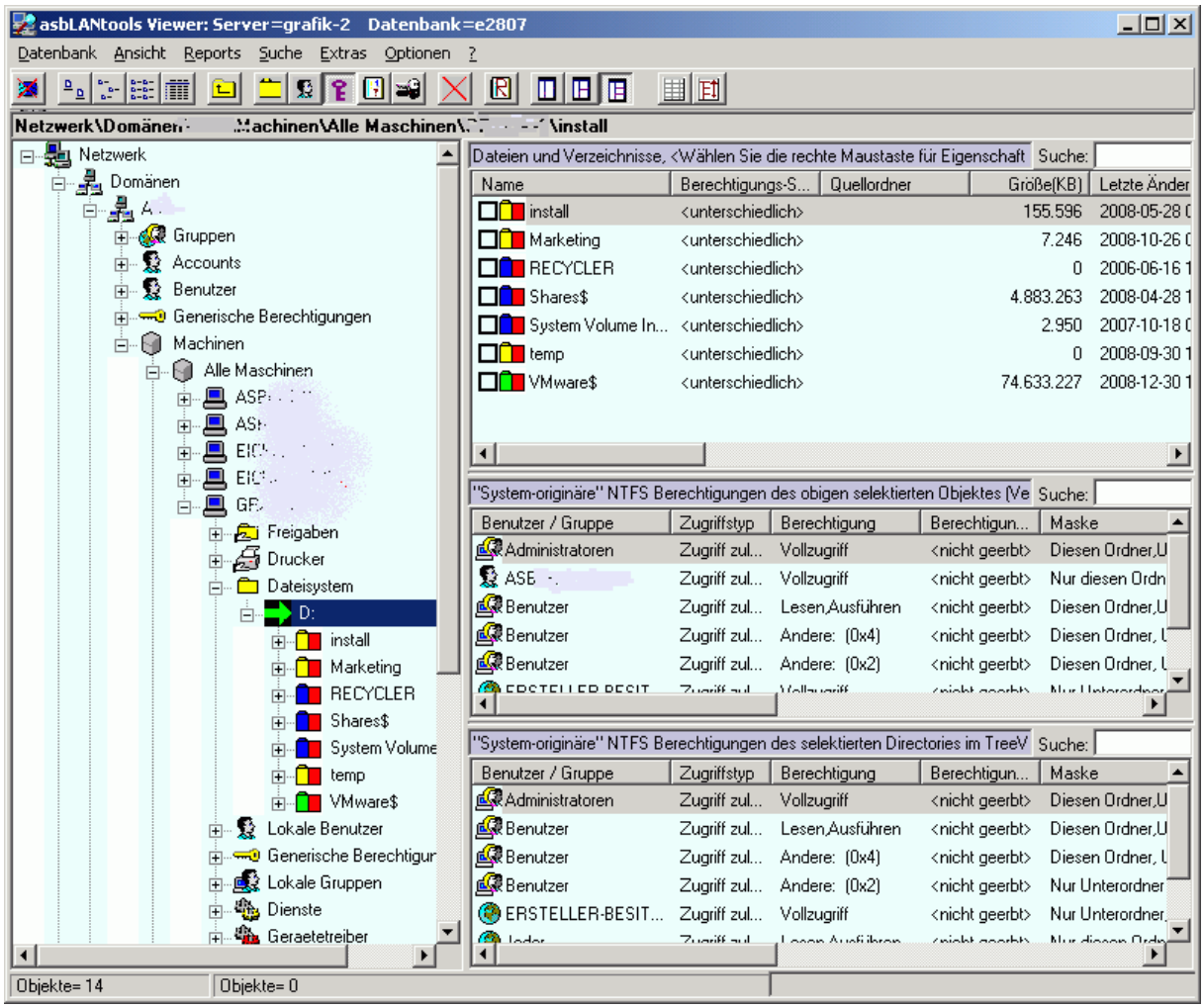


Abbildung 4.49: LTViewer mit Verzeichnisberechtigungen

Die Ikone eines Ordners im Verzeichnisbaum zeigt visuell schnell und einfach Änderungen in tiefer liegenden Strukturen an.

Welche Änderung dabei „dargestellt wird, ist im Menü Ansicht/Treeview einstellbar:

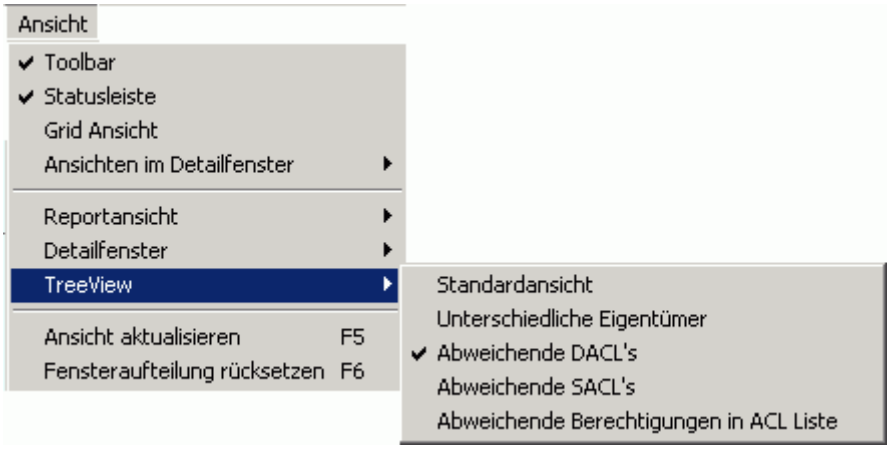


Abbildung 4.50: Menü Dialog Treeview Ansicht

Derzeit werden neben der Standardansicht abweichende DACL's/SACL's/ Berechtigungen (SACL's & DACL's) sowie Eigentümerabweichungen unterstützt:

Die Auswahl kann auch per Ikon erfolgen: Normalansicht(keine Abweichungen darstellen)/ abweichende Eigentümer/ abweichende DACL's / abweichendes SACL's in Ikonen darstellen.
Als Standard ist die Einstellung „abweichende DACL's darstellen, eingestellt.

Ikonen für Verzeichnisse haben eine 2-teilige farbige Darstellung und weisen auf folgende Informationen hin:

	Im linken Teil werden die Veränderungen in der Baumstruktur des Ordner signalisiert, d.h. jegliche Abweichung in einem „tiefer liegenden" Verzeichnis führt entsprechend eingestellter Option zu einer gelben (keine), blauen(Änderung in Objekten des Ordners) oder grünen (Änderung in tieferen Ebenen) Ikonendarstellung.
	Im rechten Teil der Ikone wird die Veränderung des Objektes selbst angezeigt, d.h. die Veränderung des Objektes zu seinem übergeordneten Objekt. Als Objekte kommen hier sowohl Dateien als Verzeichnisse in Betracht.

Tabelle 4.4: Ikonen: Baumstruktur- /Objektverhalten

Mittels dieser Darstellung kann in großen Verzeichnisbäumen sofort und unmittelbar eine optische Aussage zu Veränderungen an Berechtigungen oder anderen Abweichungen im Verzeichnisbaum getroffen werden, ohne dass alle Verzeichnisse begutachtet werden müssen

Die Ikonendarstellung findet sowohl in der Baumstruktur- als auch in den Listendarstellungen des LTViewer Anwendung. Dass Farbenspiel der Ikonen hat dabei

folgenden Bedeutung:

Ikone	Bedeutung in Baumstruktur
	Keine Änderungen im Ordner oder Unterordnern
	Der Ordner selbst besitzt Veränderungen zum übergeordneten Ordner. Es liegen jedoch keine Veränderungen im Ordner oder darunter vor.
	Im Order oder Unterordnern liegen Veränderungen vor, der Order selbst besitzt gleiche Eigenschaften wie übergeordnete Ordner
	Im Ordner sowie Unterordnern existieren Veränderungen, der Ordner selbst weist ebenfalls Veränderungen zum übergeordneten Ordner auf.
	Der Ordner besitzt Unterordner, welche Veränderungen in Unterordnern aufweisen.
	Der Ordner besitzt Unterordner, welche Veränderungen zeigen, der Ordner selbst weist Veränderungen zum übergeordneten Ordner auf. Im Ordnen selbst gibt es keine Veränderungen.
	Die Datei weist keine Veränderungen zum Ordner auf.
	Die Datei weist Veränderungen zum Ordner auf.

Tabelle 4.5: Ikonen und die Bedeutung für Verzeichnisauswertung

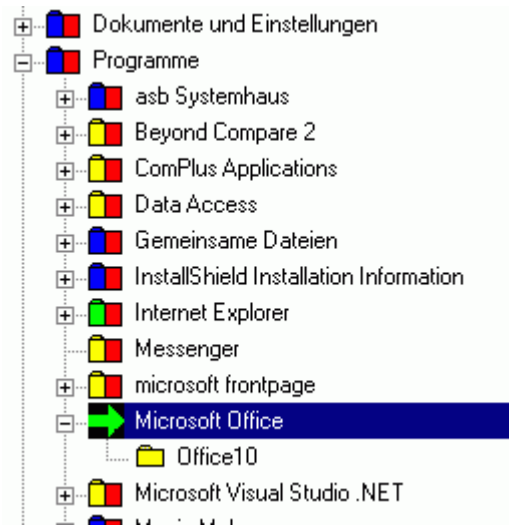


Abbildung 4.51: Verzeichnisbaum Darstellung (Auszug)

Der LTViewer zeigt in den Detailfenstern in Darstellung einer Verzeichnisstruktur folgende Informationen an:

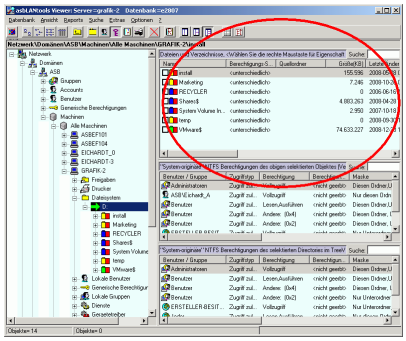
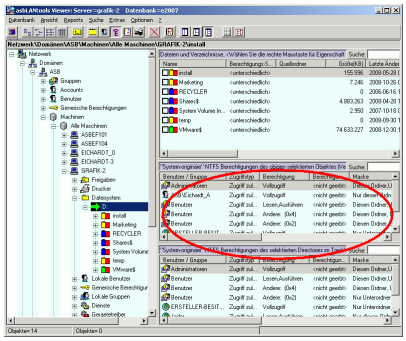
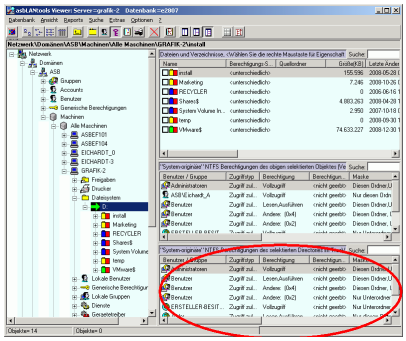
	In diesem Fenster werden standardmäßig die zum selektierten Ordner in der Baumstruktur enthaltenen Objekte (Dateien und Verzeichnisse dargestellt. Für jedes Objekt erfolgt eine Aussage zur Berechtigungs-Identität mit dem übergeordneten Ordner: <identisch>, <unterschiedlich> oder <vererbt>. Für identische und vererbte Berechtigungen wird der „Herkunftsordner“ in einer Spalte angezeigt. Status <vererbt> bedeutend, dass alle ACE’s des Objektes vererbt wurden.
	In diesem Fenster werden die Detailberechtigungen zu dem im obigen Listen-Fenster selektierten Objekt dargestellt. Zu jedem ACE Eintrag wird der ACE-Typ (Zugriff zulassen, Zugriff verbieten, Überwachung erfolgreich oder Überwachung verboten), Berechtigungsstatus (<unterschiedlich>, <identisch>, <vererbt>), die Berechtigungsmaske in normalisierter Form (Vollzugriff, Lesen, Ändern, Löschen, Andere(..))dargestellt.
	In diesem Fenster werden die Detailberechtigungen zu dem in der Baumstruktur selektierten Ordner dargestellt. (wie selektiertes Detail-Objekt) Hinweis: in asbLANtools lässt sich der Inhalt eines jeden Fensters separat steuern und verändern. Welche Informationen in welcher Abhängigkeit und welchem Fenster, Detail-Abhängigkeiten etc. dargestellt werden, ist entsprechend Kundenwunsch einstellbar.

Tabelle 4.6: asbLTViewer, List-Fenster und Inhalte für Filesysteme

Zur Anzeige in Berechtigungsdarstellungen gelangen in LTViewer derzeit nur „generische“ Darstellungen, so wie Sie im System gespeichert sind. Konsolidierende Darstellung (Zusammenfassende Berechtigungen) und anderweitige Visualisierungen sind möglich darzustellen. Dazu sind entsprechende Anpassungen, entsprechend kundenspezifischer Forderung zu tätigen.

	Berechtigungsabweichungen zwischen einem Objekt (Ordner, Datei) und seinem übergeordneten Ordner werden in asbLANtools immer nur in Bezug auf „Objekt-Berechtigungen“ ausgewertet. Objektberechtigungen stellen die „wirklichen Zugriffsberechtigungen“ für existierende Objekte dar.

Container-Berechtigungen werden „im wesentlichen“ nur für die Neuanlage eines Objekts verwendet. Ein Bespiel für somit nicht berücksichtigte Berechtigungseintragungen ist „Creater-Owner“ ACL’s, welche ausnahmslos als

Containerberechtigungen verwendet werden.

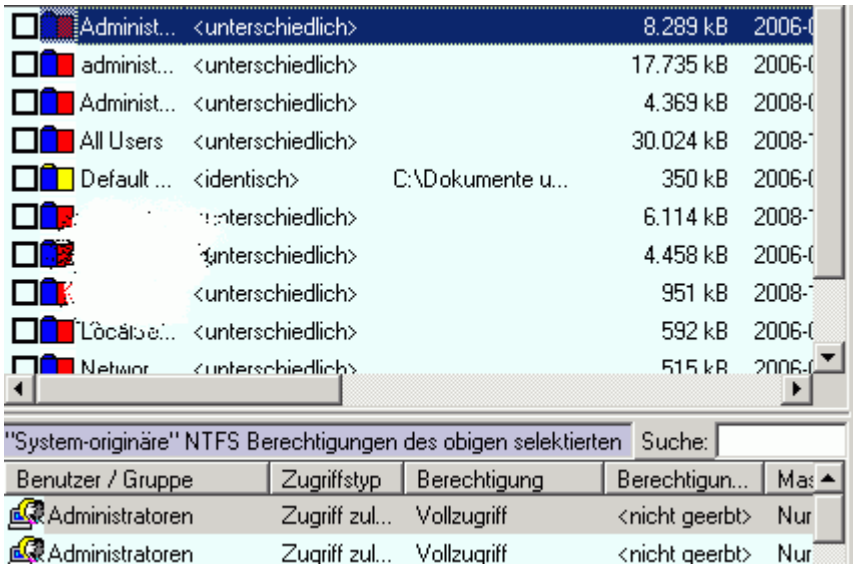


Abbildung 4.52: Berechtigungen eines Verzeichnisses

In dem Verzeichnisbaum lassen sich nun sehr differenziert Informationen betrachten: Auch zu den Verzeichnissen und Dateien kann im Kontextmenü der Befehl „Eigenschaften“ ausgewählt werden.

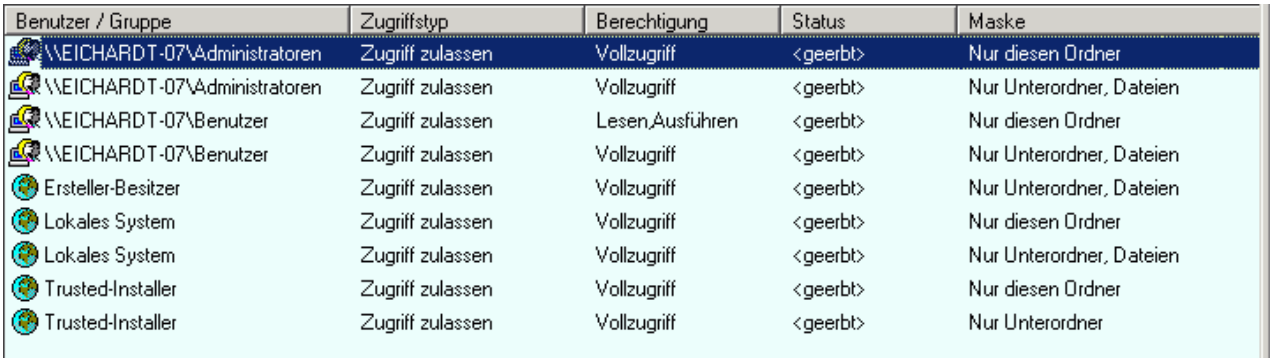
4.5.9 Filesystem /Berechtigungskonsolidierung

In der aktuellen Version wird Auswertung der Berechtigungen von Objekten für asbLANtools Benutzer durch erweiterte Berechnungen unterstützt.

asbLANtools Scan prozess erfasst alle ACL Berechtigungen in verschiedenen Darstellungen. Diese dienen dazu Zugriffsberechtigungen übersichtlich darzustellen:

Abbildung 4.53: asbLTViewer, Menüleiste mit ORC und TRC Option

- Darstellung der originären Einstellungen, wie Sie im System vorhanden sind: ORC = Original Rights Crypt;
- Darstellung der Konsolidierten Berechtigungen: KRC = Konsolidierte Rechte Crypt;
- In den asbLANtools Daten befindet sich eine weiter BerechtigungsOption: TRC = True Rights Crypt, welche jedoch nicht zur „Anzeige“ kommt.. TRC Crypt beinhaltet im Gegensatz zu KRC keine Vererbungsinformation.



Benutzer / Gruppe	Zugriffstyp	Berechtigung	Status	Maske
\\EICHARDT-07\Administratoren	Zugriff zulassen	Vollzugriff	<geerbt>	Nur diesen Ordner
\\EICHARDT-07\Administratoren	Zugriff zulassen	Vollzugriff	<geerbt>	Nur Unterordner, Dateien
\\EICHARDT-07\Benutzer	Zugriff zulassen	Lesen,Ausführen	<geerbt>	Nur diesen Ordner
\\EICHARDT-07\Benutzer	Zugriff zulassen	Vollzugriff	<geerbt>	Nur Unterordner, Dateien
Ersteller-Besitzer	Zugriff zulassen	Vollzugriff	<geerbt>	Nur Unterordner, Dateien
Lokales System	Zugriff zulassen	Vollzugriff	<geerbt>	Nur diesen Ordner
Lokales System	Zugriff zulassen	Vollzugriff	<geerbt>	Nur Unterordner, Dateien
Trusted-Installer	Zugriff zulassen	Vollzugriff	<geerbt>	Nur diesen Ordner
Trusted-Installer	Zugriff zulassen	Vollzugriff	<geerbt>	Nur Unterordner

Abbildung 4.54: Beispiel einer Original-System ACL Liste

Konsolidierte Berechtigungen ermöglichen es, die „wahren“ Zugriffsrechte von Objekten darzustellen und miteinander zu vergleichen.

Benutzer / Gruppe	Zugriffstyp	Berechtigung	Status	Maske
\\EICHARDT-07\Administratoren	Zugriff zulassen	Vollzugriff	<geerbt>	Nur diesen Ordner
\\EICHARDT-07\Benutzer	Zugriff zulassen	Lesen,Ausführen	<geerbt>	Nur diesen Ordner
Lokales System	Zugriff zulassen	Vollzugriff	<geerbt>	Nur diesen Ordner
Trusted-Installer	Zugriff zulassen	Vollzugriff	<geerbt>	Nur diesen Ordner

Abbildung 4.55: Beispiel der konsolidierten Rechte Liste

Es bestehen dazu mehrer Möglichkeiten, einer vereinfachten Darstellung:

1. Objekte vom Type Folder (Filesystem, Registry, AD..) besitzen die Möglichkeit eine Option Ihre „Wirksamkeit“ zu speichern wie „Nur dieses Object, Alle Unterobjekte usw.) In asbLAntools werde nur die „statischen“ Zugriffsrechte ausgewertet, d.h die Veranlagung bestehender Objekte und die Möglichkeit auf diese zuzugreifen.- Für die Auswertung der „Erstellung“ neuer Objekte“ müsste die Gesamtauswert wesentlich verkompliziert werden, ohne dass im Normalfall ein wesentlicher Nutzen für den Kunden zu stand kommt.
2. Durch verschiedene Manipulationen und Vorgaben für / an Objektberechtigungen kann es zu einem mehrfacheintrag ein und der gleichen Berechtigungs-ACE kommen.
3. Unterschiedlicher Vererbungszustände zweie ansonsten identischen ACE Berechtigungseinträge.

   Diese obigen Möglichkeiten werden in einem „konsolidierten“ Berechtigungseintrag berücksichtigt: Gleiche oder gleichartige Ace’s werden zusammen gefasst, Objectberechtigungen welche keinen Einfluss auf die „Statische“ Berechtigung von Objekten haben z.b: „nur Unterordner“ Option werden ausgefiltert.

   Die konsolidierte Berechtigung eines Objektes wird in wiederum in 2 Varianten gespeichert:

   - Konsolidierte Berechtigungscypt mit Vererbung
   - Konsolidierte Berechtigungscypt ohne Vererbung

   Damit ist es möglich, hinreichend genau Auswertungen in Bezug auf

Abweichungen von Berechtigungen eines Objektes im Baum zu analysieren.

Es sei angemerkt, das nicht immer alle Möglichkeiten der Gestaltung von ACE Objekten auch zu einem eineindeutigen Ergebnis zusammengefasst werde können. Die Möglichkeiten im NTFS System übersteigen bei weitem die Möglichkeiten der Darstellung.- In diesen Fall werden konsolidierten Berechtigungen so gut als möglich konsolidiert.

In Bezug auf die Vererbung von Objekten werden die folgenden Zustände für eine ACL Liste eines Objektes ermittelt:

1. Nicht geerbt, unterschiedliche Berechtigung
2. Nicht geerbt, identische Berechtigungen
3. Teilweise geerbt, unterschiedliche Berechtigung
4. Teilweise geerbt, identische Berechtigungen
5. Alle geerbt, identische Berechtigungen
6. *Alle geerbt, unterschiedliche Berechtigungen*
7. Unbekannt

Insbesondere die Aussage
Alle geerbt, unterschiedliche Berechtigungen stellt ein speziell von asbLANtools gelieferte Aussage dar, die ansonsten nicht verfügbar ist.
Dieser Fall kann auftreten, wenn ein übergeordnetes Objekt manuell mit einem weiteren ACE Eintrag erweitert wurde, dieser aber nicht vererbt wurde.

4.5.10 QueryManager

Der Querymanager als Bestandteil des LTViewers stellt ein Hilfsmittel für Support als auch ein Hilfsmittel für kundenspezifische Entwicklung von Ansichten und Reports dar.

Insofern kein anderer QueryManager (z.B. MS SQL Server) verfügbar ist, können Sie diesen für einfache Aufgeben (Abfragen) verwenden. Der im LTViewer integrierte QueryManager beinhaltet als Hilfsmittel nur eingeschränkte spezifische Möglichkeiten:

Eine Besonderheit des integrierten Querymanager besteht darin, das alle im LTViewer ausgeführten SQL Anweisungen (aus dem Viewer und Reports) an den Querymanager „gesendet werden“ können. Über Einstellungen im Menü „Option/Abfrage tunneln“, wird erreicht, dass alle ausgeführten Anfragen im Querymanager in Ihrer „aufgelösten“ Form, so wie sie an die Datenbank gesendet werden verfügbar sind.
Die im Eingabefenster selektierten SQL Anweisungen oder der gesamte Eingabetext kann über F5-Taste ausgeführt werden, jedoch immer nur eine Abfrage.

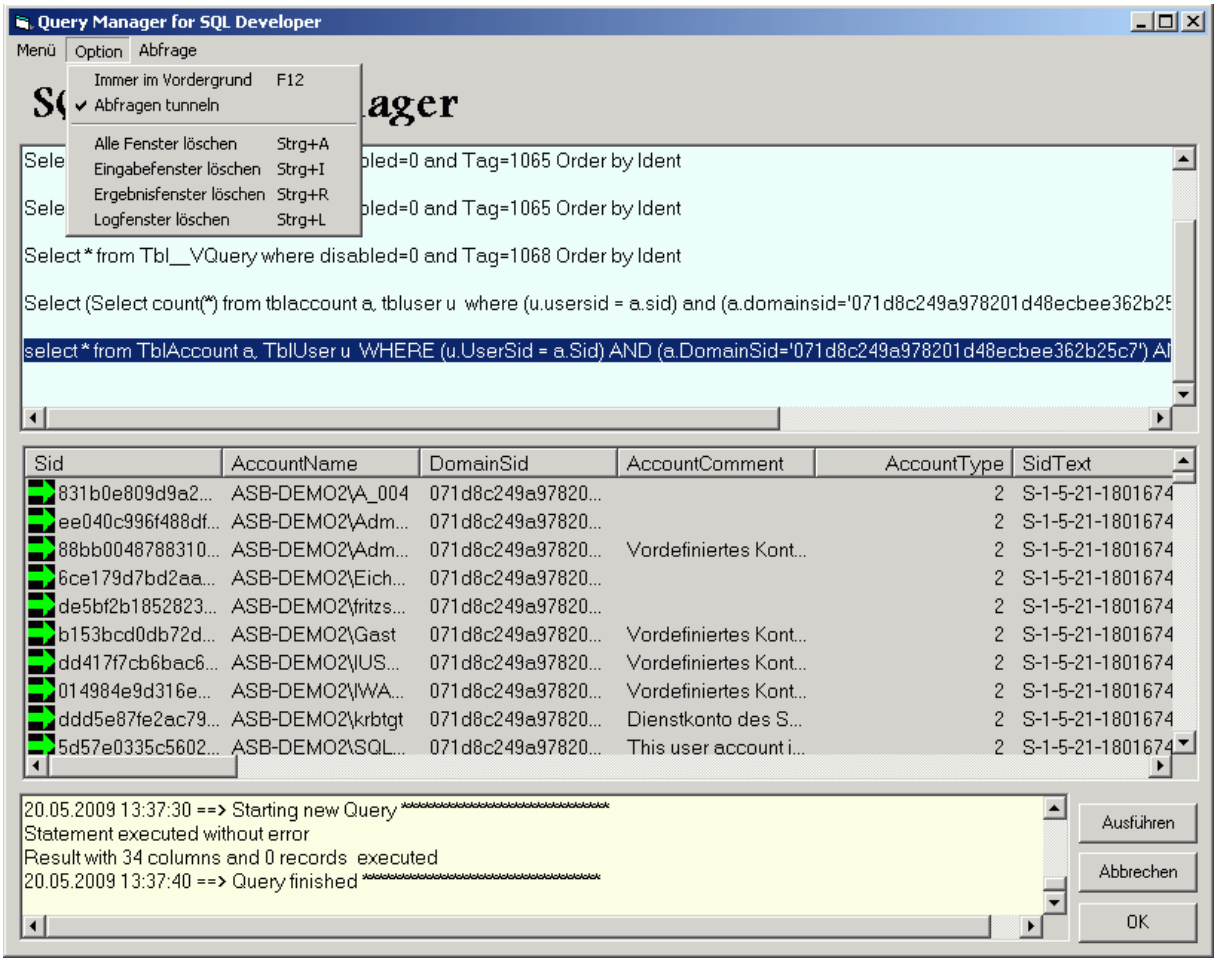


Abbildung 4.56: Querymanager

4.6 Reports

asbLANtools beinhaltet ein leistungsfähiges Reporting. Dies kann über das Modul LTViewer gerufen werden.

Mit der aktuellen Version sind ca. 100 Standard-Reports verfügbar.
Die Reports werden in 2 unterschiedlichen Kategorien wie folgt genutzt:

- Netzwerkreports
  werden über Menü Viewer/Reports aufgerufen.
  Diese Reports (Type „N“) betreffen immer den gesamten Datenbankinhalt. Viele inhaltliche gleichwertige Reports finden Sie auch als „selektive Reports vor.
- Selektive Reports
  werden immer über eine selektierte Datenmenge im LTViewer, Fenster 2 (siehe Kapitel Viewer/Oberfläche) mittel der rechten Maustaste gestartet.

Die vollständige Übersicht über alle verfügbaren Reports, finden Sie in dem Dokument **Report-Uebersicht.PDF** im Ordner „\Documents“.
Muster-Ausgaben finden Sie im Ordner Musterreports.

Report Vorlagen befinden sich im Unterverzeichnis Reports des Installationspfades. Diese können hier flexibel ergänzt oder verändert werden. Nicht benötigte Reports

können gelöscht werden. Veränderte kundenspezifische Mengen-Auswahl lässt sich durch die im RDF Reportfile hinterlegte Abfrage steuern.
Ein Report wird über seinen Dateinamen, welcher auch in den Menüs und im Report sichtbar ist, selektiert werden.
Zu einem Report gehören jeweils eine Datei vom Typ .RDF und .RPT.
Im Reportverzeichnis vorhandene Files werden beim Start des Viewers auf ihre Verwendbarkeit geprüft (oder auch Menü Viewer/ Report aktualisieren) und in der aktuellen Anwendung sodann registriert.

Werden Reports hinzugefügt, geändert oder gelöscht, so wird die interne Reportliste des asbLAN*tools* Viewer bei jedem Neustart oder über das Menü „Reports“/ „Aktualisieren“ erneuert.

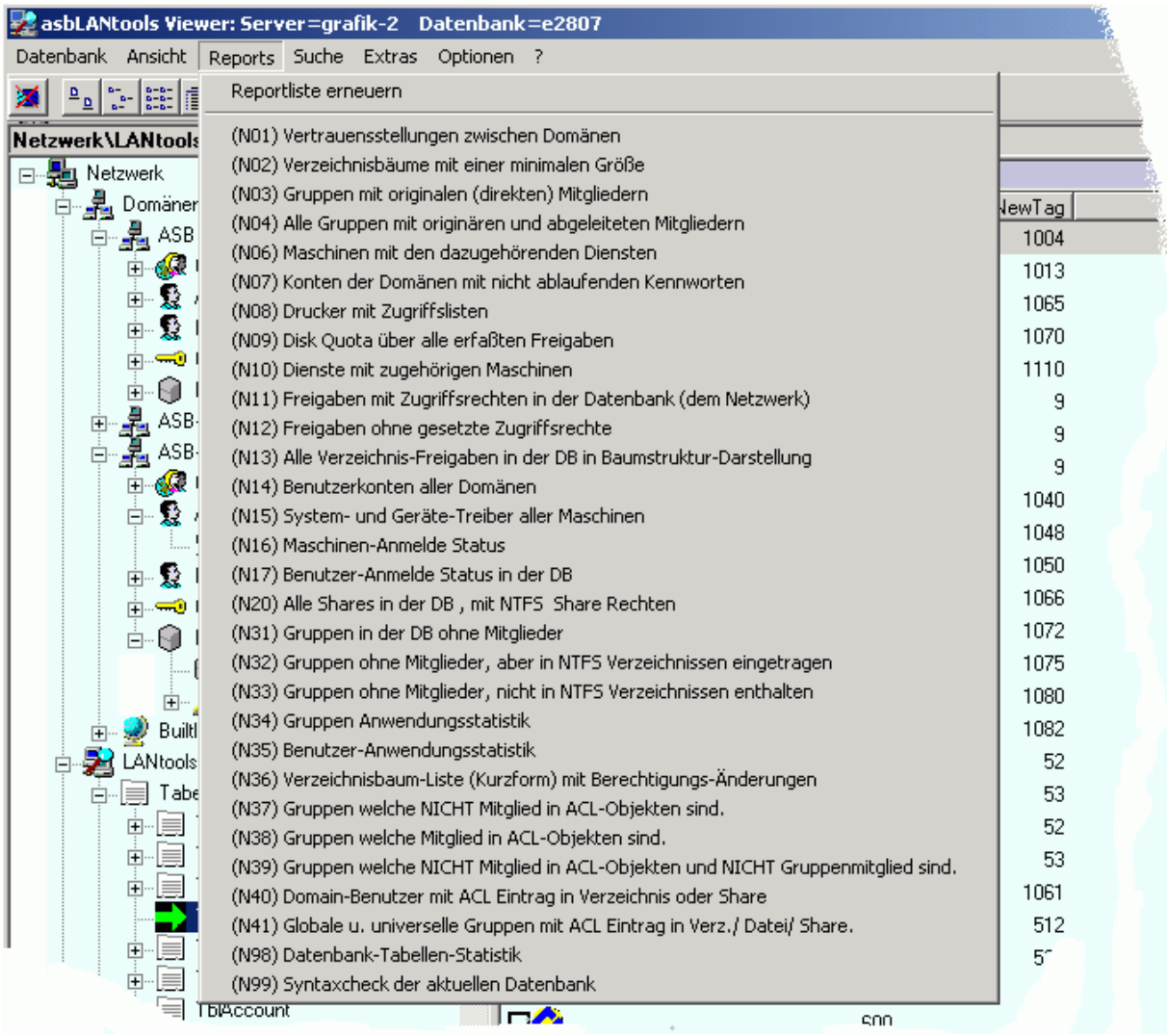

asbLANtools Viewer: Server=grafik-2 Datenbank=e2807
Datenbank Ansicht Reports Suche Extras Optionen ?
Reportliste erneuern
(N01) Vertrauensstellungen zwischen Domänen
(N02) Verzeichnisbäume mit einer minimalen Größe
(N03) Gruppen mit originalen (direkten) Mitgliedern
(N04) Alle Gruppen mit originären und abgeleiteten Mitgliedern
(N06) Maschinen mit den dazugehörenden Diensten
(N07) Konten der Domänen mit nicht ablaufenden Kennworten
(N08) Drucker mit Zugriffslisten
(N09) Disk Quota über alle erfaßten Freigaben
(N10) Dienste mit zugehörigen Maschinen
(N11) Freigaben mit Zugriffsrechten in der Datenbank (dem Netzwerk)
(N12) Freigaben ohne gesetzte Zugriffsrechte
(N13) Alle Verzeichnis-Freigaben in der DB in Baumstruktur-Darstellung
(N14) Benutzerkonten aller Domänen
(N15) System- und Geräte-Treiber aller Maschinen
(N16) Maschinen-Anmelde Status
(N17) Benutzer-Anmelde Status in der DB
(N20) Alle Shares in der DB , mit NTFS Share Rechten
(N31) Gruppen in der DB ohne Mitglieder
(N32) Gruppen ohne Mitglieder, aber in NTFS Verzeichnissen eingetragen
(N33) Gruppen ohne Mitglieder, nicht in NTFS Verzeichnissen enthalten
(N34) Gruppen Anwendungsstatistik
(N35) Benutzer-Anwendungsstatistik
(N36) Verzeichnisbaum-Liste (Kurzform) mit Berechtigungs-Änderungen
(N37) Gruppen welche NICHT Mitglied in ACL-Objekten sind.
(N38) Gruppen welche Mitglied in ACL-Objekten sind.
(N39) Gruppen welche NICHT Mitglied in ACL-Objekten und NICHT Gruppenmitglied sind.
(N40) Domain-Benutzer mit ACL Eintrag in Verzeichnis oder Share
(N41) Globale u. universelle Gruppen mit ACL Eintrag in Verz./ Datei/ Share.
(N98) Datenbank-Tabellen-Statistik
(N99) Syntaxcheck der aktuellen Datenbank
Netzwerk\LANtools
Netzwerk
NewTag
1004
1013
1065
1070
1110
9
9
9
1040
1048
1050
1066
1072
1075
1080
1082
52
53
52
53
1061
512
TblAccount

Abbildung 4.57: Network Reports

Das in asbLANtools integrierte Reportsystem basiert aktuell auf Crystal Reports System(CR) der Firma SAP, vormals Business Objects und zuvor als Seagte Software (Crystal Reports) bekannt..
Das implementierte Interface ermöglicht die Nutzung der Möglichkeiten des CR Systems zur Voransicht, Auswahl, Ausgabe, Druck, Suche und Darstellung.
Generell wird mit Ausführung eines Reports dieser in einer Minimalansicht innerhalb des Hauptfensters LTViewer integriert dargestellt.

Nach der Auswahl von Objekten und dem Aufruf eines Reports wird dieim LTViewer

integrierte „minimale“ Ansicht aufgerufen. Sind keine Datensätze für die Report Ausgabe verfügbar erfolgt eine Mitteilung.

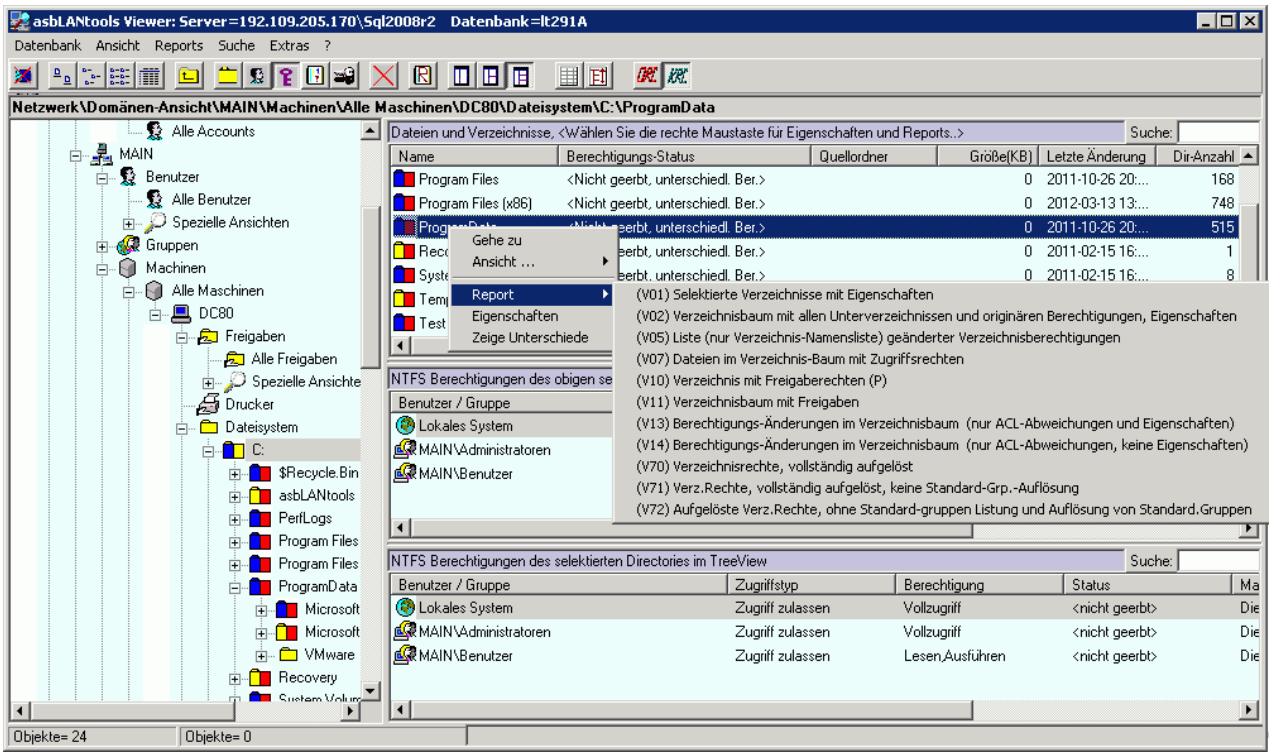
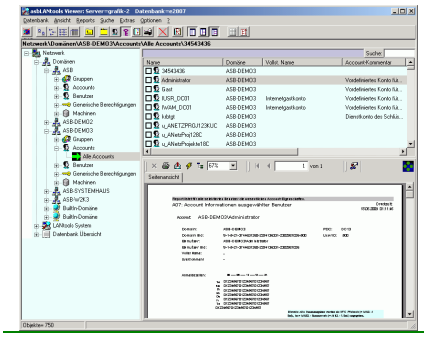


Abbildung 4.58: Auswahl eines selektiven Reports für ausgewählte Objekte

Für die Auswahl von Objekten können die Windows-typischen Funktionen <Strg> und <Shift>-Taste sowie Bereichsmarkierung verwendet werden.

Anschließend wird der Reports Kontroll-Dialog mit dem Bericht geöffnet. Sie können sich den Bericht dort betrachten, aus diesem Fenster heraus die Druckausgabe auf den definierten Standarddrucker über das Drucker-Symbol starten oder den Bericht in verschiedene Dateiformate exportieren, filtern, indexiert betrachten oder nach speziellen Informationen suchen.

Ein Report kann innerhalb von LTViewer die folgenden unterschiedlichen Ansichten, je nach Erfordernis an die Aufgaben, einnehmen:



Reportansicht, nach dem Aufruf eines Reports: Ein Report wird nach dem Aufruf immer in den LTViewer Detailfenstern F2 und F3 (siehe Bedienoberfläche). eingeblendet. Als Nutzer können Sie zwischen verschiedenen Reportansichten umschalten.

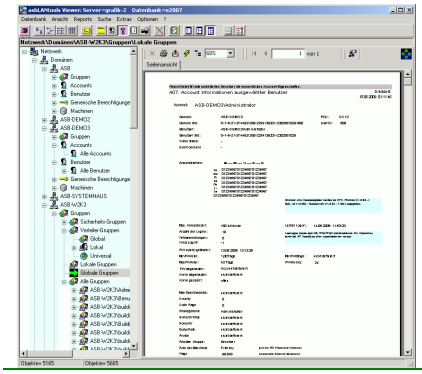
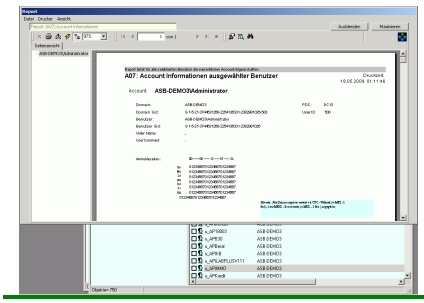
	Zum Umschalten der Ansicht eines Reports haben Sie mehrere Möglichkeiten: - „R“ Taste im Menü von LTViewer schaltet die Ansicht des Reports weiter. - Menübefehle Ansicht/Reportansicht, sowie die - Tastensteuerung für eine Reportansicht <Strg> F4, <Shift> F4,.. <Shift> F7>
	Ansicht eines Reports in einem externen Fenster. Als weitere Möglichkeit können Sie die Reportansicht ausblenden, oder schließen (aus dem Speicher entfernen).

Tabelle 4.7: Reportansichten im LTViewer

Beispiel einer Reportansicht in einem externen Report-Fenster:

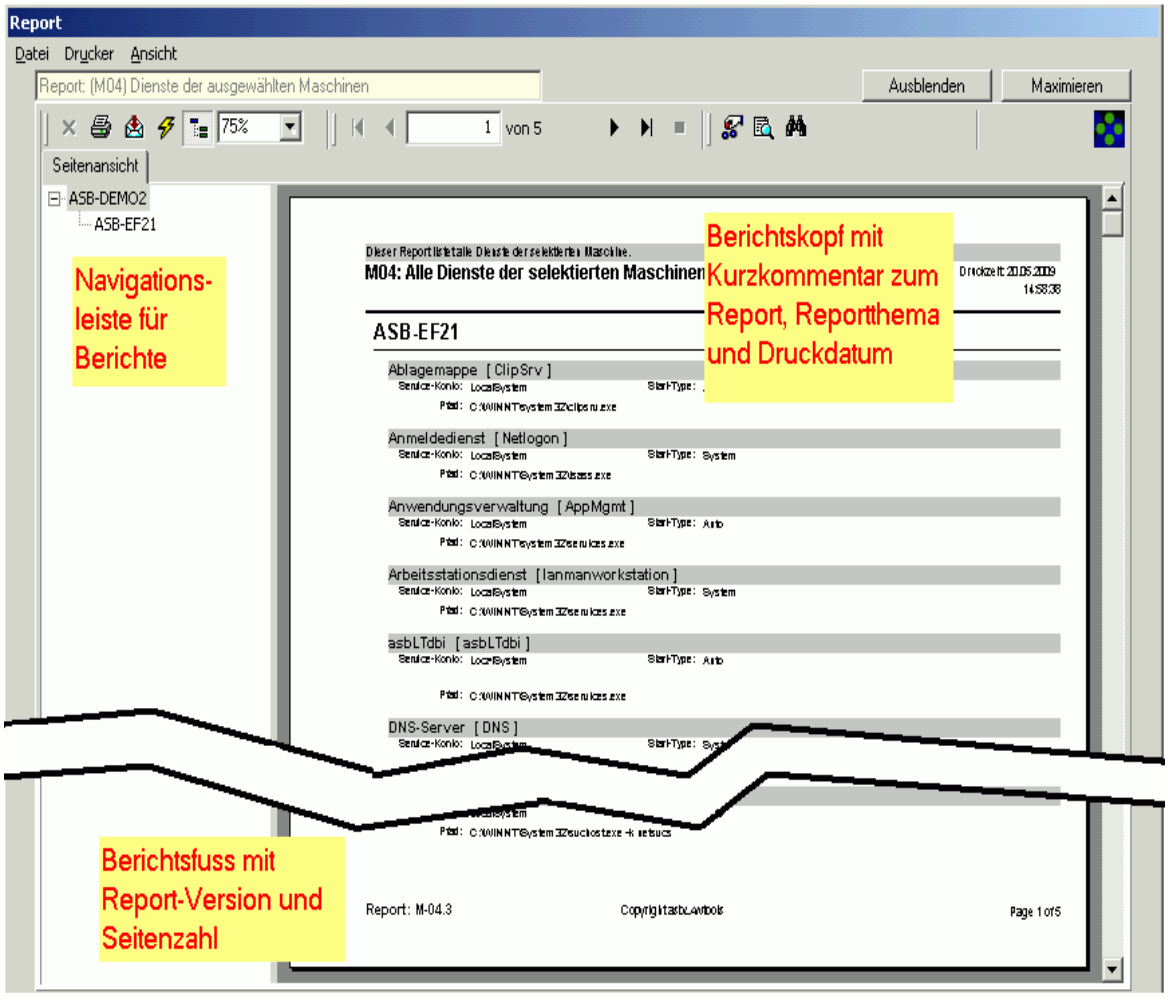


Abbildung 4.59: Report-Layout Struktur

4.6.1 Übersicht Reports

Die Übersicht der verfügbaren Reports wird ständig erweitert und aktualisiert. Diese finden Sie in der Datei **Report_Uebersicht.pdf** im Ordner „\Documents“ der asbLANtools Installation oder auch im Web www.asb-systemhaus.de.

Die Reportverarbeitung erfolgt nach dem folgenden Schema:

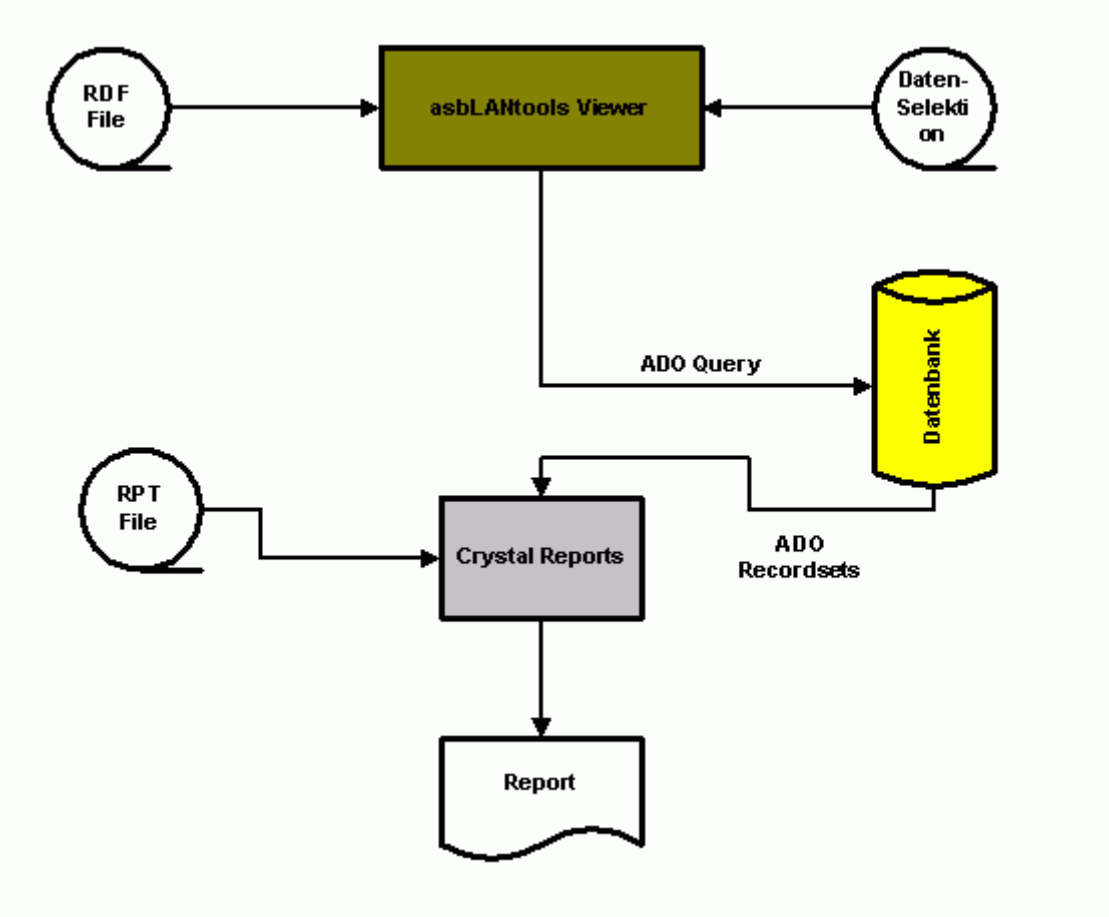


Abbildung 4.60: Report Verarbeitung, Schematische Darstellung

4.6.2 Arbeiten mit Reports

Der Umgang mit Reports der asbLANtools erfordert einigen Aufwand, sowie auch einige Erfahrungen im Umgang mit den eigenen Daten. Auf Grund der unterschiedlichen Gestaltung der Kunden-Netzwerke ergeben sich aus den Datenbeziehungen auch recht unterschiedliche Verhaltensweisen einzelner Reports.

Anbei erhalten Sie einige praktische Hinweise, welche Sie unbedingt beachten sollten.

Reports anpassen

Sie haben die Möglichkeit bestehende Reports anzupassen, oder neue Reports hinzuzufügen. Die Anpassung von Reports ist nicht Gegenstand dieses Handbuches. Lesen Sie dazu im Technischen Handbuch nach.

Große Datenbanken, Datenmengen

Die Ausführungszeit zur Darstellung eines Reports kann recht unterschiedlich ausfallen. Es existieren Reports, welche in wenigen Sekunden „mehrere Hundert Seiten“ generieren, oder aber auch durchaus 30 min für einen komplexen Report benötigen, je nach Datenmenge, bereitgestellte Datenbank-Serverleistung und Komplexität des Reports.

Für die Arbeit und den Umgang mit Reports müssen Sie Ihre eigenen Erfahrungen mit Ihren Daten sammeln.
An den Datenbankserver übergebene Abfragen können erst unterbrochen/ abgebrochen werden, wenn dieser eine Rückmeldung bringt.

Abfrage liefert keine Daten

Für Abfragen, welche ein „leeres“ Ergebnis, d.h. kein zur Abfrage passenden Daten liefert erfolgt der Hinweis per Hinweis-Fenster:

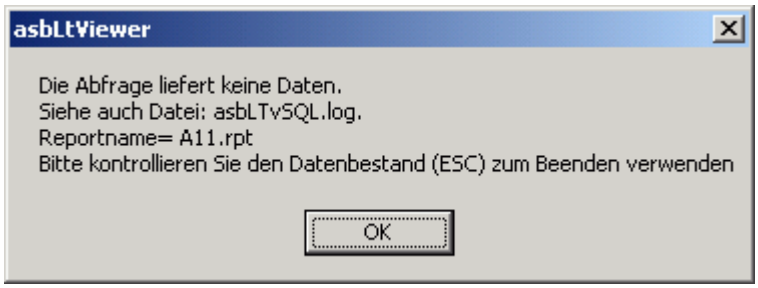


Abbildung 4.66: Reportaufruf , keine Daten

Die Ursachen für einen „leeren“ Report können recht unterschiedlich sein. Wählen Sie die folgende Vorgehensweise:

- Überprüfen Sie, ob die für diesen Report erforderlichen Daten überhaupt in der Datenbank existieren (hauptsächlicher Fehler). Dazu haben Sie die Möglichkeit der Ansicht „Import- Daten“ sowie Tabellenansichten als auch die Möglichkeit Detaildaten in verschiedenen Strukturen zu sichten.
- Beachten Sie bitte die Abhängigkeit von Informationen siehe Kapitel 1, Konzept.
- Prüfen Sie ob die Daten ohne Fehler importiert wurden (Logprotokoll).
- Prüfen Sie, ob die importierten Daten bereits Fehler in dem DatenScan hatten (Scan Fehler, verschiedener Ursachen)
- Überprüfen Sie die Abfragen. Nutzen Sie dazu den integrierten QueryManager (Einstellung Abfrage tunneln, nutzen).
- Senden Sie ihr Problem an asb Systemhaus Support.

Report Logging

Alle vom Bediener aufgerufenen Reports (Report-Anweisungen) werden in einem separaten Logfile im Ordner "\Log\asbLTvSQL.Log“ gespeichert. Die verwendeten Eingangsdaten (aufgelöste SQL Syntax) für den Report können somit nachvollziehbar in einem SQL Querymanager getestet werden. Siehe auch vorherige Kapitel.

4.7 Modul Batch-Prozessor (asbLTcmd)

Die Verarbeitung von Aufträgen kann alternativ zum Modul Administrator, manuell auch über den asbLTcmd Batch-Prozessor erfolgen.

Die Syntax des Batchprozessor asbLTcmd ist ab Version 2.7.0.8 geändert worden. Bitte korrigieren Sie ggf. Ihre Batch-Prozeduren, welche asbLTcmd benutzen.

Generell wurde die neue Syntax an allgemein gültigen Eingabesyntax von Windows ausgerichtet: Kommando /Optionsname und Parameter/ Dateneingabe wurden durch „Abstandszeichen“ voneinander getrennt, Beispiel Scan einer Domäne

Alte Syntax(V 2.8): asbLTCmd –s“D dom-01“ => ein Parameter

Neue Syntax(V 2.919: asbLTCmd –scan „D dom-01“ => zwei Parameter

Befehle können in der neuen Syntax in Langform oder eingekürzt eingegeben werden.

Die Syntax selbst ist selbsterklärend und wird in dem Inline Help des Programms gepflegt: Aufruf asbLTCmd -?

Nachfolgend ist die Syntaxstruktur von asbLTcmd wie in der integrierten Hilfe beschrieben:

Program call: asbLTCmd <command> [<parameter> [<parameter>]] [/option..]
<command> : starting with “-“ or “/”
<parameter> : any data
========= ========================

- Taskfile <TaskFile[.LTB]> Use task-file
- Execute <TaskList> Execute task (Scan data and Import into default db)
- Scan <TaskList> Scan task; Ex.:“-s “D my-dom;F \\Dc01\C$; M \\DC01”
- Import [<FromFolder>] Import data from “Folder” or from working directory
- SetDB [<db>] Set default database key= [”A”..”Z”]
- ShowDB Show default database setting
- ClearDB [<db>] Clear database
- DBSTAT Statistic for selected database
- ? ,-Help Show this helpfile

Options:

- DATABase <db> or - DB <db> Use specifed database “A”,...”Z” for DB Import
- Workdir <WorkDir> Optional directory for Temp-/Output-Scan files
- PROfile <IniFile> Use Profile instead of registry for asbLTCMD proc.
- Debug <hex> Show additional information
- Verbose Show all process information
- TRace Show detailed information
- PRIo <Prio> Run with spec. priority -2,-1,0,1,2, default=0

Command-Language:

- no difference between lower and upper chars
- It’s possible to reduce a command for example: Execute, Execut, Execu, exec, ex or e

```
Format specification for <TaskList> parameter:
TaskList          = "<task>; [<task> ] [;..]"       // one or more tasks enclosed within double-breakets
                                                    // and separted by semicolon
Task              = <TaskType <TaskName> [/TaskOption]>
TaskType          = "D" | "F" | "M"  | "L"
TaskOption        =  </OptionName> [<space <value>] [/Taskoption] [„„]
Example:
  "D <domain-name>"          // Scan/Import Domaine                  example: "D my-dom"
  "M <machine>"              //Scan/Import Machine                  example:  "M \\Server01"
  "F  <share>"               // Scan/Import Share/Folder    example: "F \\SERVER-1\C$"
  "L <LDAP Profile>          //  LDAP Scan mit vordefinierten AD Path, Properties und Filtern;

asbltcmd -e "D asb /Prio 3; M \\Server01; F \\Server\C$; TaskName Server_C"
        => or use this input from <Taskfile> as same content from TaskFile: "Scan.LTB":
   D asb /Prio 3          //Scan Domain "asb" with priority=3
   M \\Server01           //Scan Server01
   F \\Server\C$          //Scan Filesystem C$
<eof>

// data from Scan will be imported to default db (-execute) instead of (-scan) only
asbltcmd -Taskfile scan.ltb        //Start asbLtcmd with input from TaskFile

Using <IP-Adress> instead of Netbios Name or DNS-Name:
   D 192.100.100.1            //Scan Domain from dc with specified IP Adress
   M \\192.168.2.1            //Scan server with IP 192.168.2.1
   F \\92.168.2.1\C$          //Scan files from share C$ of IP.
```

Abbildung 4.67: asbLTCmd, integrierte Hilfe

4.8 Profiler Version

Die asbLANtools asbLTcmd Ausgabe als Profiler Version stellt eine im Wesentlichen der CMD (Batch-Prozessor) adäquate Nutzung Version dar. Alle Informationen werden in einer INI (Profile Format) Datei gespeichert.
Die Profiler Version gestattet es asbLANtools Daten für den mobilen Einsatz zu erfassen:

- Revisionsaufgaben
- Scannen von Teilnetzwerken
- Serviceleistungen (Dienstleister)

Datenbank basierende Aufgaben werden mit der Profiler Version nicht unterstützt, bzw. sind nicht vorgesehen.

Die Nutzung von asbLTcmd als Profile Version erfolgt durch Eingabe des Zusatzoption

cmd> asbLTcmd /Profile <profile.ini>

In der Profile Datei sind alle Nicht-Standard-Angaben zwingend erforderlich, zu definieren. Auszug aus einer Profile Steuerdatei:

```
[Description]
//asbLANtools Registry-Profile: Reg_Profile_Muster.INI
//Stand: 2011/08/09

[Parameters]
// Dieses Profile kann mit Parameter-Werten zur einfacheren Arbeit mit Daten gestaltet werden
// Es ist möglich sich wiederholende Angabe wie FilePath, Reg-Key  durch %Parameter%
// Darstellungen wie in diesem Beispiel zu gestalten.
// Beispiele
// in den einzelnen Daten-Abschnitten werden sodann Werte mir Parametern wie folgt dargestellt:
// [%p1%]
// [%p1%\Administrator\Parameters]
//=> Parameter ermöglichen eine effektive Verwaltung der Profile;
// 1)Wichtig: auf abschliessende "\" achten im Parameterfeld !!
// 2)[Parameters] Section muss vorn an im Profile.ini stehen; (Zuerst eingelesen werden)
//
// Erweiterungsmöglichkeiten: p1,.., pN
//
P1=HKEY_LOCAL_MACHINE\SOFTWARE\asb Systemhaus\asbLANtools\Version_291
P2=C:\Programme\asb Systemhaus\asbLANtools291

[%P1%]
Language=00000001
ScriptPath=%P2%\Script_Output
password=
Blocksize=00000064
InitPassword=
..
[%P1%\Administrator\Parameters]
ScanFiles=00000001
LogFile=%P2%\log\asbLANtools.log
```

```
DebugLevel=00000000
LDAP=00000001

 [%P1%\Generic Keys]
LogPath=%P2%\Log\
InstallPath=%P2%\
ReportPath=%P2%\Reports\
ViewPath=%P2%\Views\
Language=00000001
DC_Type=80080018

[%P1%\License]
License=asbLANtools 0291U2012065000  unlimited     Unlimited Testlizenz;;;
Key=fccd2d34a9a0ea2774cb89f11a2e20a6....
LicenseFile=%P2%\License_291.lic
```

Abbildung 4.68: asbLTcmd Profile Steuerdaten

4.9 asbAD Active Directory Dump Service

asbAD.exe ist ein Zusatzmodul für die Dump-Ausgabe der gesamten oder auszugsweisen Darstellung von Daten des Active Directory.

asbAD arbeitet mit vorkonfigurierten Einstellungen in einem Config-File.
Diese können sie auch für den AD/LDAP Scan innerhalb von asbLANtools verwenden.

Dies bietet den Vorteil, dass bei der Vielzahl der Möglichkeiten „Aufgaben“ komplett in einem Profile abgelegt werden.

asbAD kann somit als Bestandteil der asbLANtools (Ausgabe der Daten in Tabellen, welche eine Treeview Struktur des AD abbilden) oder separat über asbAD.exe im Dump-Format, genutzt werden.

Voraussetzung für die Nutzung von asbAD ist eine gültige asbLANtools Lizenz.

asbAD ermöglicht die Selektion in mehreren Ebenen sowohl auf Hierarchie-Ebene als auch als Auswahl der auszugebenden Eigenschaften.

Alle Daten werden in einem druckbaren, übersichtlichen Profile-Format ausgegeben. In jedem Fall, auch bei Selektion einzelner Objekte aus einem AD Baum wird eine rückwärts verzeigerte Struktur ausgegeben. Dies ermöglicht den Vergleich verschiedener Ausgaben sowie die maschinelle Verarbeitung der Daten in externen Programmen;
Neben „allen“ im AD verfügbaren Eigenschaften, welche generisch ermittelt werden , wird auch die Berechtigung von Objekten vollständig ausgegeben.

AsbAD Profile Vorgaben lassen sich auch direkt in einen DatenScan von asbLANtools mit anschließenden DB Import verwenden. Siehe dazu Abschnitt „Daten scannen“.

asbAD wird über CMD Interface gestartet:

CMD> asbAD.EXE DUMP <ProfileName.INI>

Die Standardausgabe der Daten erfolgt über Standardoutput und kann mit

CMD> asbAD DUMP <ProfileName.INI> >> Output.Dat

in eine Datei umgeleitet werden;

Die Möglichkeiten der asbAD Analyse sind vielfältig. Insbesondere können LDAP-Search-Strings, die Darstellung der Objektklassen, Eigenschaften je Objektklassen und Text-Ausgabefilter sehr einfach eingestellt werden.

Die vollständige Funktionsbeschreibung eines Profiles finden Sie unter Documentation\Example_LDAP.INI. Anbei ein Musterbeispiel, Auszug aus einem Profile zur Steuerung eines LDAP-Scan:

```
// Stand: 2012/03/20

[$generic]
Description         = asb-Test Domain
//Provider          = LDAP:
Provider            = GC:
//Path              = Rootdse
//Path              = OU=Alfons_Unit,OU=Test,OU=asb_Test,DC=Main,DC=T2k8R2,DC=de
Path                = DC=Main,DC=T2k8R2,DC=de
Server              = dc80
SEARCHPREF_SEARCH_SCOPE         = SubTree
//SEARCHPREF_SEARCH_SCOPE       = OneLevel
SEARCHPREF_PAGESIZE             = 1000
SEARCHPREF_SIZE_LIMIT           = -1
Filter              = (ObjectClass=*)
//Filter            = ( & (ObjectClass=user)(CN=Eller_2))
//Filter            = (ObjectClass=user)
//Filter            = (& (CN=eich*) (ObjectClass=User) (!ObjectClass= computer)  (!Memberof=*test*) )

[$Filter]                                                   //Object-String-Filter
//distinguishedName             = OU=Test
//Member                        = Eller_2
//Name                          = Eller_2           //Filter für alle Objekte der OU... oder OU=abc,OU=  ...
                                                    //-> Exakt "Sub-String" Vergleich beachten !!
//OBJECTSID                     =S-1-5-21-2947777159-912655230-2867235419-1105

[$DefaultObjectClass]                       /Print [$Defaultproperty] for this class, * = All Classes
*                                           //print All classes
//User

[$DefaultProperty]                          //Print Property  for Default Objectclass
*                                           //Print All properties for all "printable" classes
$Class
$ObjectID
ObjectGuid
$ParentGuid
$ADsPath
$Availabe Properties
$Read Properties
$ParentAdsPath
$CollectTime
$ObjectOwner
```

```
$ObjectSecurity
$Comment
$Schema
//$SidCrypt
//$AclList
//$Available Values
CN
distinguishedName
//ObjectClass
ObjectGuid

[User]                  //Print selected Property for specified class (user),
*                       //= print all prop. for user
ObjectSID
Name
[//Comment_Key]         //Dieser key wird samt aller Properties ignoriert;
Ignored_Property
[-Ende]                 //"-„   => "Eingabe-Ende; Nachfolgende Eingaben werden ignoriert;
```

Abbildung 4.69: Auszug aus einer Profile Steuerdatei für den LDAP Scan

Die Ergebnisse eines AD/LDAP Scans werden in einer Textdatei oder Standard-Output gespeichert:

```
[$Start_1c8c8f487a644e2b9cf6a472f6a275ed]
*** asbAD, Dump utility for Active Directory, type "?" for more help ***

==> Start Reading LDAP Data with profile: b:\test_Dc80.ini

-->         Start reading AD data with ADSI/LDAP scanner
<started>   Start LDAP search process
                Search Options:
                SuchStrategie   = Tree-Suche
                Search_Limit    = -1
                SearchPageSize  = 500
12:17:57.427(UTC-Time)

            List of LDAP search tasks:
                Provider        = "LDAP://"
                Server          = "dc80/"
                Init-DN         = "DC=Main,DC=T2k8R2,DC=de"
                Filter          = "(ObjectClass=*)"
12:18:00.12 (UTC Time);Search process finished, object infos loaded; Used time = 3 sec.
            Number of found objects= 224;
<started>   Build_Map ...
12:18:00.12 (UTC Time) Please wait ...
<finished>  "Build_Map process"23:18:04.71 (UTC-Time);
<started>   Select_Property process started;
12:18:04.71 (UTC Time) Please wait ...

[09ce6924e42e8844a2dd224074e5acec]
$Availabe Properties      = 14
$Read Properties          = 14
$Availabe Values          = 15
$Class                    = container
$ObjectID                 = 123
$CollectTime              = 2
$AdsPath                  = LDAP://dc80/CN=0b7fb422-3609-4587-8c2e-94b10f67d1bf,
                                CN=Operations, CN=DomainUpdates,CN=System,
                                DC=Main,DC=T2k8R2,DC=de
$ParentAdsPath            =
LDAP://dc80/CN=Operations,CN=DomainUpdates,CN=System,DC=Main,DC=T2k8R2,DC=de
$ParentGUID               = 4f64b5663aa5a74b803d8f6f1227b3f8
$Schema                   = LDAP://dc80/schema/container
```

```
CN                          = 0b7fb422-3609-4587-8c2e-94b10f67d1bf //!  (AT:3 / VT:8)
DISTINGUISHEDNAME           = CN=0b7fb422-3609-4587-8c2e-94b10f67d1bf,CN=Operations,
                                CN=DomainUpdates ,CN=System,DC=Main,DC=T2k8R2,DC=de
                                //!  (AT:1 / VT:8)
DSCOREPROPAGATIONDATA       = 1601-01-01 00:00:00.000 //!  (AT:9 / VT:7)
INSTANCETYPE                = x00000004= 4 //!  (AT:7 / VT:3)
NAME                        = 0b7fb422-3609-4587-8c2e-94b10f67d1bf //!  (AT:3 / VT:8)
NTSECURITYDESCRIPTOR        = x033371d4 //!  (AT:25 / VT:9)
$ObjectOwner                = Domänen-Admins
$ObjectSecurity(00-00);     = x00(Zugriff erlaubt);            für Dieses_Objekt;
                                Authentifizierte Benutzer;      00020094(Lesen);
$ObjectSecurity(00-01);     = x00(Zugriff erlaubt);            für Dieses_Objekt;
                                Domänen-Admins;                 000e01bf(Vollzugriff -
                                (Objekt_Löschen+Unterstruktur_Löschen));
$ObjectSecurity(00-02);     = x00(Zugriff erlaubt);            für Dieses_Objekt;
                                SYSTEM;                         000f01ff(Vollzugriff);
$ObjectSecurity(00-03);     = x12(Zugriff erlaubt);   Geerbt;  für Alle_Objekte;
                                Administratoren; 000f01bd(Objekt_Listen+Ordner_Listen
                                +Alle_Best_Schrebvorgänge+Rechte_Lesen+Prop_Lesen+Sub-
                                Obj_Erstellen+Prop_Schreiben+Rechte_Schreiben
                                +Besitzer_Ändern+Objekt_Löschen+Erw.Prop_ändern);
$ObjectSecurity(00-04);     = x12(Zugriff erlaubt);   Geerbt;  für Alle_Objekte;
                                Organisations-Admins;           000f01ff(Vollzugriff);
OBJECTCLASS(00)             = top //!  (AT:3 / VT:8)
OBJECTCLASS(01)             = container //!  (AT:3 / VT:8)
OBJECTGUID                  = 09CE6924E42E8844A2DD224074E5ACEC //!  (AT:8 / VT:17)
SHOWINADVANCEDVIEWONLY      = true //!  (AT:6 / VT:11)
USNCHANGED                  = x00000000000016b1; 1601-01-01 00:00:00.000
                                //!<SystemTime or LongLong> //!  (AT:10 / VT:9)
USNCREATED                  = x00000000000016b1; 1601-01-01 00:00:00.000
                                //!<SystemTime or LongLong> //!  (AT:10 / VT:9)
WHENCHANGED                 = 2011-02-15 16:30:36.000 //!  (AT:9 / VT:7)
WHENCREATED                 = 2011-02-15 16:30:36.000 //!  (AT:9 / VT:7)

[391891cb7d088d40815cc25798d06ac5]
$Availabe Properties         = 14
$Read Properties             = 14
$Availabe Values              = 15
$Class                        = container
$ObjectID                    = 70
$CollectTime                 = 2
$AdsPath                     = LDAP://dc80/CN=0e660ea3-8a5e-4495-9ad7-ca1bd4638f9e,
                                 CN=Operations,CN=Domain ..

….
```

Abbildung 4.70: Auszug aus einer LDAP Dump Ausgabe

Obige Ansicht wurde zu besseren Lesbarkeit formatiert.

Alle gefundenen Objekte und Eigenschaften werden in Form einer Profile Struktur in Textform gespeichert. Die Ergebnisse können einfach über einen Script weiter verarbeitet werden. Ein Ergebnis wird immer rückwärts verkettet über „$ParentGuid“ und „$ParentAdsPath“ bis zum jeweiligen Domain-DNS Objekt ausgegeben.

4.10 Modul ScanService

Der ScanService ist eine leistungsfähige Komponente zur automatisierten Datenerfassung. Über das Administrator-Menü asbLTS Admin können alle Parameter eingestellt werden.

Einsatzhinweise über die Zusammenarbeit von ScanService und Datenimport finden Sie im Kapitel 5.2.

Weitere Hinweise zum Einsatz in großen Netzwerken, Gestaltung in WAN Netzwerken etc. finden Sie im Kapitel 2.4.

Der ScanService wird zur Einrichtung aller notwendigen Einstellungen über das Programm asbLTs.exe gestartet. Zuvor müssen Sie jedoch dem Dienst-Konto von asbLTS (siehe Dienste Manager) ein Konto zuweisen, welches die erforderlichen Berechtigungen zum DatenScan besitzt. Dies ist ein Domain-Admin Konto! Günstiger weise richten Sie für asbLANtools ein eigenes Servicekonto ein, welches keine Berechtigung zur interaktiven Anmeldung besitzt.

Der Programmaufruf kann über das Menü „asbLANtools Overview“, sowie „Startmenü/Programme/asb Systemhaus/asbLANtools“ erfolgen.

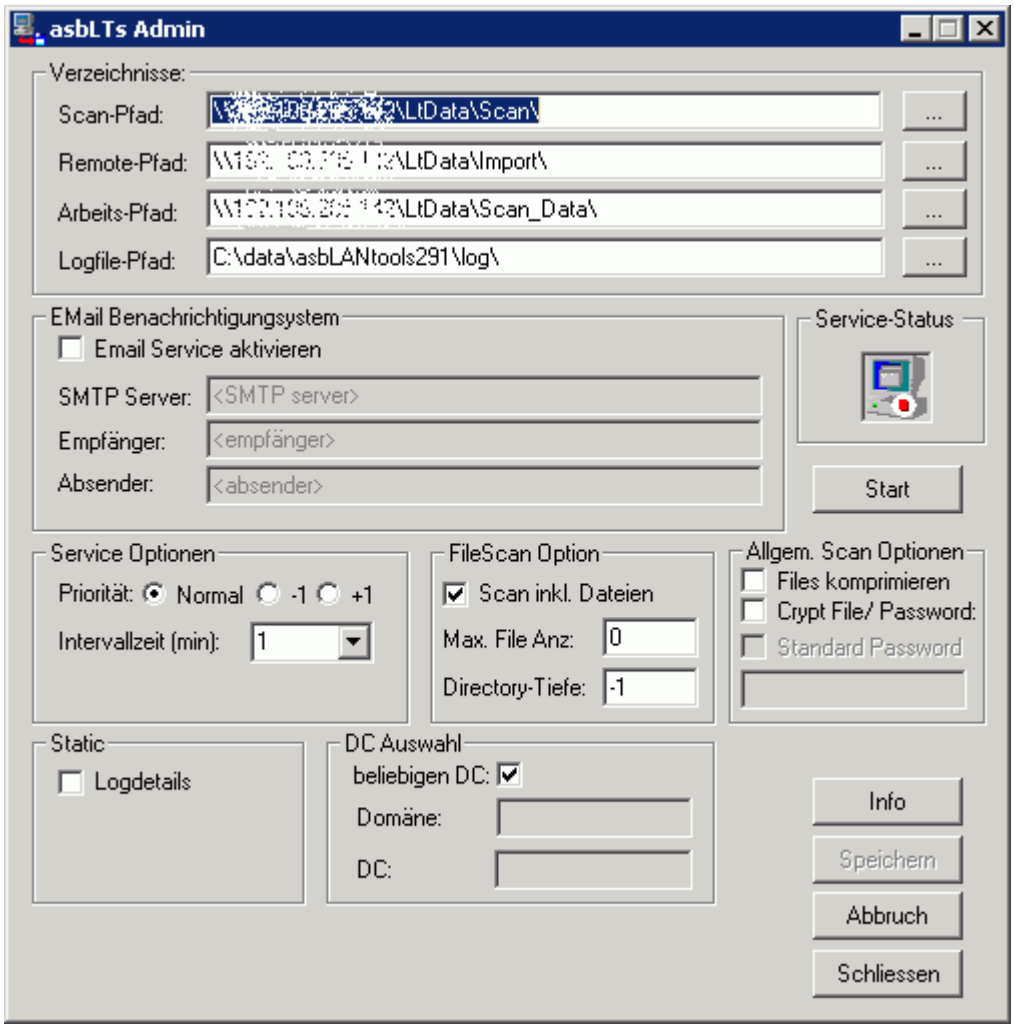


Abbildung 4.71: Modul ScanService

Erforderliche Einstellungen:

- Pfad für Auftragsdateien (Scan);

- Pfad für Zielserver (Remote);
- Pfad für Logfile;
- Pfad für Arbeitsverzeichnis;

Optionale Einstellungen:

- Mail-SMTP Einstellungen:
  SMTP Server; Empfänger und Absender Adresse;
  Falls keine Fehlernachrichten per SMTP gesendet werden sollen, geben Sie jeweils „." für SMTP-Server und Adresse ein.
- Intervall: Default=1 Minute
  Intervall, in welchem der Auftragsordner nach neuen Aufträgen durchsucht wird.

Arbeitsverzeichnis:

Der ScanService verwendet das Auftragsverzeichnis (siehe Pfad für Auftragsdateien) auch als Arbeitsverzeichnis (Stammverzeichnis).

Vorgangsbeschreibung eines Scanprozess:

Der ScanService ist auf maximale Sicherheit ausgelegt. Die Zuordnung der Ein-Ausgabeordner kann lokal als auch über Shares in einem Netzwerk erfolgen. Zielsetzung ist, jederzeit einen eindeutigen Bearbeitungs-Zustand zu erzeugen.

Der gestartete Scan Service überprüft zyklisch das „Auftragsverzeichnis" nach vorliegenden Aufträgen (*.LTB Files) im als Scan-Path einstellbaren Ordner.

Mehrere vorliegende Aufträge werden nacheinander verarbeitet. Es kann nur ein ScanService je System/ Rechner installiert standardmäßig werden.

Nach der Bearbeitung eines Auftrages wird

- LTX Datenfile
- SLOG Logdatei
- LTB Batchdatei

aus dem „Arbeitsbereich" des LTScan Services in das „Import Verzeichnis" des Import Services verschoben.

Abgebrochene Aufträge werden bei Neustart (Restart) des Scan Service erneut verarbeitet.
Der ScanService erzeugt eine LOG Mitteilung im zentralen Logfile des Scan Services, oder sendet ein voreingestellte Mail, bei Fehlern.

4.10.1 Dateistrukturen für einen Scan Auftrag

In der aktuellen Version wurden die Steuerdateien auf ein Minimum reduziert.
Ein Job wird ausschließlich in einer LTB Auftragsdatei, bestehend aus einer Task-Liste definiert. Job und Task-Einträge erhalten im Verarbeitungsprozess eineindeutige Spezifikationen (GUID's), welche eine Nachvollziehbarkeit überall und jederzeit vom Auftrag bis zum Report ermöglichen.

Beispiel für eine Auftragsdatei vom Typ LTB:

```
D Domainname            //Domäne über Domian Name erfassen
D 192.158.2.1           //Domäne über DC erfassen
M \\Server1             //Serverdaten über Maschinen-Name erfassen
M \\192.168.1.1         //Maschine übe IP Adresse erfassen…
F  \\Server1\fibu       //Filesystem über Share Spezifikation erfassen
F  \\110.100.100.10\UserData  //dto. Share über IP Adresse erfassen.

L C:\Data\AD_Profile.INI      //LDAP Profile Steuerfile
```

Eine LTB Datei besteht aus einer Standardtext Datei mit einem oder mehreren Zeilen.

Einzelne Aufträge zum Scannen von Informationen (bestehend aus Domäne | Server | Share-File Information) können in der LTB Datei gespeichert werden.

Es können folgende Task-Typen verarbeitet werden:

- „D“ Domain
- „M“ Maschine
- „F“ Filesystem
- „L“ LDAP

Task-Anweisungen in beliebiger Reihenfolge und Anzahl in einer Datei vorkommen. Wichtig: Die Hierarchie „D“ „M“ und „F“ muss mindestens zur Zeit der Auswertung in einer Datenbank gegeben sein; Der SCAN einzelner Task („D“, „M“, „F“, „L“) kann zu unterschiedlicher Zeit, unterschiedlichen Jobs und Prozessen /Maschinen erfolgen.

Die Eingabe der IP Adresse kann an beliebiger Stelle anstatt des NetBios Namens innerhalb von asbLANtools erfolgen.
Anstatt des Domänen-Namens kann ein DC angegeben werden, dann werden alle Informationen von diesem DC ausgelesen.

Eine Auftragsdatei (LTB) kann von

- Administrator
- Batch-Prozessor (asbLTcmd)
- Scan Service

gleichermaßen verarbeitet werden.

4.11 Modul Import Service

Der Import Service bietet eine automatisierte Möglichkeit des Imports gescannter Daten in eine Datenbank.

Der Import Service wird separat analog dem ScanService administriert. Der Service überwacht ein „Import-Verzeichnisbaum“ auf neuere Daten. Die Überwachung erfolgt zyklisch, einstellbar.

Vor dem Start des Import-Services müssen Sie jedoch dem Dienst-Konto von asbLTImport (siehe Dienste Manager) ein Konto zuweisen, welches die erforderlichen Berechtigungen zum Schreiben in die Datenbank(en) und Schreiben des Import Logfiles ermöglicht. Hierzu können Sie günstiger Weise das gleiche Konto wie für den

DatenScan nutzen, oder ein separates Konto erstellen. Günstiger weise richten Sie für asbLANtools ein eigenes Servicekonto ein, welches keine Berechtigung zur interaktiven Anmeldung besitzt.

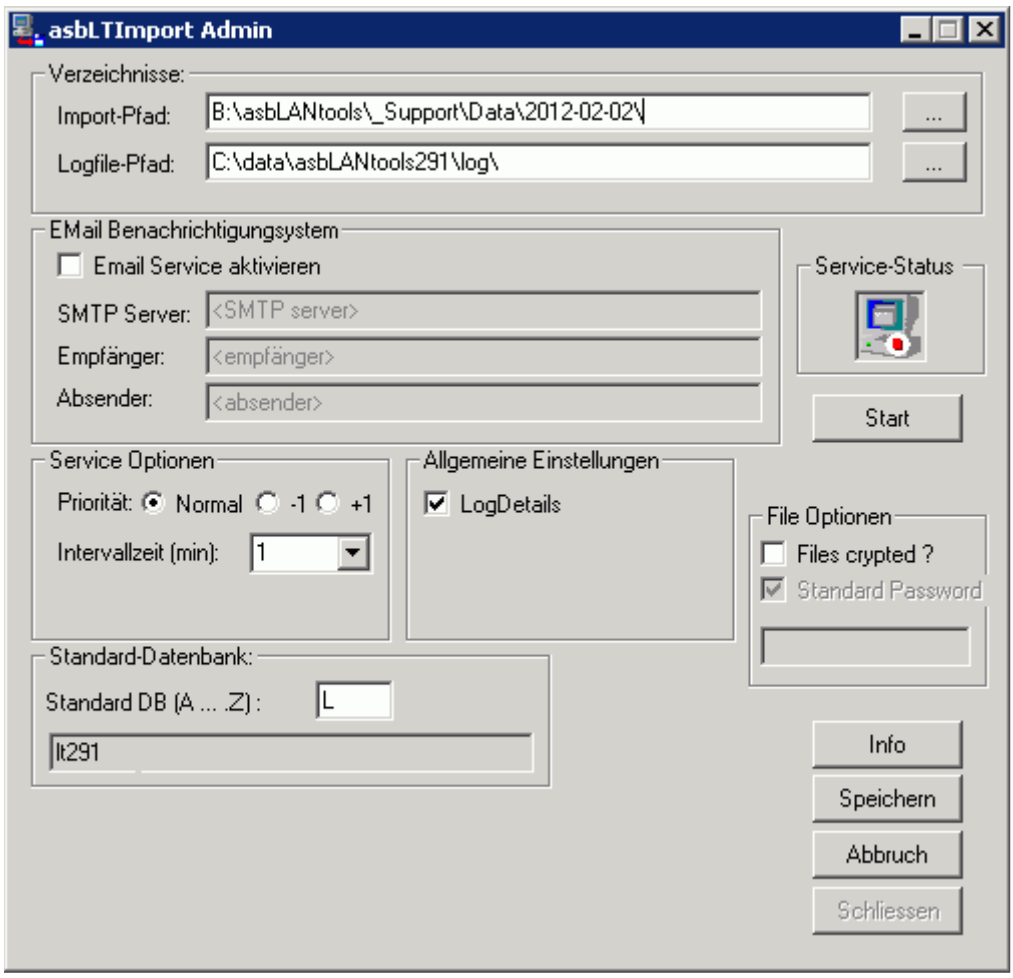


Abbildung 4.72: Modul Import Service

Überwachtes Verzeichnis:

Die zu importierenden Daten werden aus diesem Verzeichnis oder „Verzeichnisbaum“ importiert.

Protokolldatei:

Ein Logprotokoll informiert über alle Aktivitäten des Importservices.

Starten des Dienstes:

Vor dem Start des Dienstes sollten Sie sich über die Einstellungen des asbLTdbi Dienstes vergewissern und folgendes prüfen:

Zuweisung eines Dienstkontos:

Notwendige Rechte für ein überwachtes Verzeichnis sind „Schreib“ Rechte.

Zugriffsrechte auf die Datenbank:

SQL Server Kono mit Schreibrechten in die Datenbank.

Auswahl der Import-Datenbank:

Die zu nutzende Datenbank kann über Kurzeingabe der DB Definition a... z eingegeben werden. Der DB Displayname wird im Klartext angezeigt.

Daten-Cryptierung:

Zur Sicherung der asbLANtools Scan Ergebnisse in Dateien vom Typ LTX oder LTX.GZ können diese Daten zusätzlich gegen unbefugten Zugriff durch Codierung geschützt werden. Der Importprozess muss dabei die gleichen Codierungs-Regeln wie der Scan Prozess verwenden. Diese Einstellungen sind beidseitig manuell vorzunehmen.

Hinweise: Vergessene Passwörter können nicht reaktiviert werden.

In der aktuellen Version wurden Änderungen in der Datenstruktur, Ablage und dem Datenimport vollzogen. Der Import Service importiert automatisch alle Daten des „Import-Ordners“ in die vordefinierte Datenbank. Wird diese zwischenzeitlich gelöscht, soll schreibt der Import Service die Daten wieder in die DB.

Die Einstellungen des asbLTImport und asbLTScan Services sind von den Einstellungen des LTAdmin und asbLTCmd Modules unabhängig.

5 asbLANtools anwenden

5.1 Konfigurationshinweise

5.1.1 Festlegung eines Domaincontroller (DC) für den Scanprozess

Zur Beschleunigung eines Scans kann ein DC je Domäne in der lokalen Arbeitsumgebung fest eingestellt werden. Bei Auswahl eines DC werden die Daten zwangsläufig von diesem DC erfasst. Tragen Sie dafür Sorge, dass diese Maschine auch verfügbar ist. Die Einstellungen können auch direkt in der Registry voreingestellt werden.

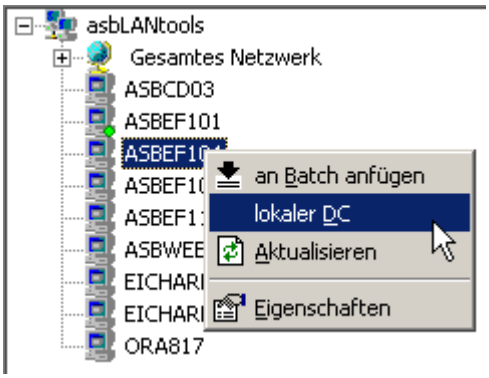


Abbildung 5.1: Auswahl eines Domänencontrollers für den Scan Prozess

Die Auswahl eines DC erfolgt über die rechte Maustaste. Ein ausgewählter DC wird mittels Ikone gekennzeichnet (PC mit grünen Punkt).

Die Festlegung eines DC's für den Scanprozess kann auch Domänen basierend in der Registry verankert werden. Dazu speichern Sie unter
HKLM/Software/asb Systemhaus/asbLANtools/Version_291/Domain-Controller
für den jeweiligen Domain-Namen den zugehörigen DC als String-Eintrag.

Der hier verankerte DC wird sodann vorzugsweise für die jeweilige Domäne verwendet.

5.2 Daten importieren

Der Datenimport stellt einen neuralgischen Punkt der Software dar. Im Standardablauf, bei fehlerfreier Installation der Datenbank, Datenbank-Zugriffs-Software (ADO, SQL/OLEDB, sowie der asbLANtools Datenbank lassen sich asbLANtools Daten problemfrei in eine Datenbank importieren.
Probleme treten erfahrungsgemäß vorrangig dann auf, wenn

a) Installations- und Kompatibilitäts-Probleme vorliegen;
b) Der DatenScan fehlerhafte Daten erstellt hat;
c) Der Datenspeicher des SQL Servers nicht ausreicht, oder lizenzseitig, bzw.

anderweitig eine SQL Server Begrenzung vorliegt (Express Version...).
Altdaten der Versionen 2.8 können problemlos in die aktuelle Version einer Datenbank importiert werden. Es kann jedoch durch fehlende Detailinformationen (Erweiterungen der akt. Software) zu Ansichts- und Auswertedefiziten kommen.

In der vorliegenden Version wird für jeden Datenimport ein separates Protokoll geführt.
Der gesamte asbLANtools-Prozess von DatenScan bis zum Datenimport kann über Prozess-variablen kontrolliert werden, sodass die Datenherkunft in der Auswertung eineindeutig nachvollzogen werden kann.
Insbesondere sind somit Aussage über Datenbestände einer DB derart möglich, dass rückwärts die Herkunft der Daten ermittelt werden kann (Wann wurden die Daten erfasst, wann wurden die Daten zur Auswertung in die DB importiert).

In der aktuellen Version werden vor der Ausführung des Datenimports eines Task-Bestandes diese auf Fehler geprüft. Fehlerhafte Daten(Tasks) werden nicht, bzw. nicht automatisch übernommen. Diese Einstellung kann manuell geändert werden.

Somit wird z.B. verhindert, dass nach einem „routinemäßigen" DatenScan Altdaten in einer DB überspielt werden, wenn Teile des neuen Scan-Jobs (einzelne Task Ergebnisse) fehlerhaft sind. Der Import eines, ist Fehlern behafteten Datenscans kann aber z.B. im Modul Administrator manuell angestoßen werden, sodass die nur fehlerfreien Task Ergebnisse importiert werden.

Hintergrund dieser Regel ist die vollständig automatisierte Übernahme von Daten in eine Datenbank (sie Import Service), sowie die bevorstehende Einführung eines Versions-Managements.

5.3 Automatisierte Datenerfassung

Eine automatisierte Erfassung und Bereitstellung von Daten durch asbLANtools ist mit dem Einsatz der Services DatenScan (asbLTS) und ImportService (asbLTdbi) gegeben.

Mit der Einführung von Prozess-Transaktionsnummern können sowohl mehrere Scan- als auch Import-Services parallel auf eine oder mehrere Datenbanken arbeiten.
Widersinnige Aufträge wie das „parallele" Erfassen und importieren gleicher Auftragsinhalte sollte vermieden werden (Ein Job importiert Daten, während der andere Altdaten für einen Import löscht usw...).
Zu importierende Tasks werden an Hand Ihrer Transaktionsnummern (Scan/Import, Scan/Import Datum und Task-Auftrag) verifiziert. Die qualitative saubere Domain-Zeit sollte auf allen beteiligten Systemen gegeben sein. Seitens asbLANtools wird dies kontrolliert und ggf. der Prozess unterbrochen (Delta 15 min).

5.3.1 Datenbank Import-Service

Je Datenbank und „Import-Server“ ist sollte max. ein „Import-Service“ installiert sein. (Mehrfach Services sind manuell installierbar).
Damit können beispielsweise parallel erfasste Sub-Domain, oder umfangreiche Fileserver auch parallel in eine oder mehrere Datenbanken installiert werden.

Der DatenScan legt in der aktuellen Version alle Daten (LTX Files) in einem Verzeichnis ab. Der Import-Services besitzt die Eigenschaft, das Import-verzeichnis und die ausgewählte Datenbank miteinander abzugleichen und fehlende, neuere Daten wieder in die DB zu importieren. (So entsteht der Nebeneffet, dass über den LT Administrator gelöschte DB’s wieder automatisch gefüllt werden, wenn der Import-Service im Hintergrund nicht angehalten wird.

5.3.2 Datenfluss bei Scan- und Import-Service

Für die Anwendung der automatisierten Erfassung(Scan) und DB Import empfiehlt sich die Einrichtung der folgenden Directorys, wobei darauf zu achten ist, dass die Dienste die Verzeichnisse erreichen können und Schreibberechtigungen aufweisen. Die Verzeichnisse können menügesteuert eingerichtet werden.

- Scan Vorbereitung:
  In diesem Verzeichnis sollten alle Jobs für den Scan Prozess gepflegt werden. Es ist ein Scheduler Prozess einzurichten, welcher die Jobs, in das vom Scan-Service überwachte Verzeichnis kopiert.
- Scan:
  Das Verzeichnis dient als überwachtes Auftragsverzeichnis. Alle hier gespeicherten Aufträge werden vom ScanService in das Arbeitsverzeichnis (ScanDatum) verschoben und ausgeführt.
- ScanData:
  Dieses Verzeichnis beinhaltet aktive als auch inaktive Daten eines Scan-Prozesses. Nach der ordnungsgemäßen Ausführung wird das Verzeichnis bereinigt.
- Import:
  Ein erfolgreich ausgeführter Scan-Job wird in das überwachte „Import-verzeichnis“ transportiert und hier gespeichert. Der Import Prozess prüft die Daten im „Importfolder“ und importiert „jeweils“ neuere Scandaten in die Datenbank.
  Der Datenbestand des Import-Verzeichnisses ist manuell oder skript-basierend zu pflegen. Derzeit werden hier keine Eingriffe durch einen asbLANtools Prozess vorgenommen.

5.3.3 Große Netzwerke

Bei großen Netzwerken ist der „Erfassungsaufwand“ entsprechend hoch. Deshalb kann es vorteilhaft sein, mehrere Teil-Aufträge zu organisieren. Auf jedem Rechner, der geeignet ist einen „Service“ zu starten kann ein asbLANtools Scanprozess oder /und ImportService eingerichtet werden. Der Offline – Scanprozess kann mit dem Task – Scheduler unter Verwendung einer Batchdatei mit „asbLTCMD.exe“ oder dem ScanService automatisiert werden. Nachdem der Scan erfolgreich beendet wurde, erfolgt ein Kopiervorgang zum „Import-Folder“ auf welchen der Import Service zugreift

.

Für die Anforderungen der Datensicherung sollten die „gescannten“ Ergebnisse in die erforderliche Datensicherung einbezogen werden. Möglichkeiten dazu bieten sich auf Grund des modularen Konzeptes von asbLANtools ausreichend an.

5.4 Dezentrale Erfassung

Der Einsatz der asbLAN*tools* in einem WAN stellt keine Probleme dar. Um die Belastung der WAN – Strecke zu umgehen, ist es möglich die Domänendaten von beliebigen, oder zielgerichtet von einem vorbestimmten DC zu scannen. Bevor ein Sammelprozess mit dem Administrator gestartet wird, ist über ein Popup – Menü, welches über einen Klick mit der rechten Maustaste auf den DC (Klick auf die Maschine im linken oberen Fenster) erreichbar ist, die Wahl „lokaler DC“ möglich. Die angewählte Maschine wird in der Registry eingetragen und bei jedem neuen Sammelprozess verwendet.

Ein anderes Konzept die WAN - Strecke zu umgehen, besteht darin den Sammelprozess vom Import in die Datenbank zu trennen. Mit asbLAN*tools* werden die gesammelten Daten in Textdateien geschrieben bevor sie in die Datenbank importiert werden. Bei einem Offline – Sammelprozess fällt der Import in die Datenbank weg und die Textdateien können in einer belastungsfreien Zeit zum Datenbankserver kopiert und erst dort importiert werden.

Für die Definition eines Auftrages kann folgender Syntax (siehe auch Scan-Syntax) verwendet werden:
“D <Domäne>“ oder „D </<DC>“, bzw. „D <DC-IP-Adresse>“

Für die Verbindung zu einer entfernten Domäne /Maschine ist ggf. eine IPC$ Verbindung über „NET USE“ einzurichten. Seitens asbLANtools werden auf Grund interner Anforderungen sodann die Verbindungen automatisch vervollständigt (Es sind sowohl IPC Verbindungen über IP als auch Hostnamen, je nach Aufgabe erforderlich).

6 Tabellen und Übersichten

Die folgenden Dokumente und Übersichten sind Bestandteil des Produktes asbLANtools:

- Datenbankmodell , siehe technisches Handbuch
- Reportübersicht, siehe Anlage
- Scan Filestruktur , siehe technisches Handbuch
- Registry Einträge
- Fragen und Antworten

DB Modell, Tabellen, Script, Registry und weitere Übersichten und Details sind Bestandteil des technischen Handbuches.

6.1 SQL-Skripts

asbLANtools verwenden zur Realisierung verschiedener Auswertungen eine Vielzahl von SQL Scripts (Prozeduren, Funktionen und Sichten).
Zur Gewährleistung der Systemstabilität werden Scripts standardmäßig nicht ausgeliefert, bzw. frei gegeben.
Die vorhandenen Skripts können jedoch zur Gestaltung eigener Auswertungen für Modul Viewer als auch für die Reportgenerierung genutzt werden.

Skripts werden mit einer „vordefinierten MDF SQL Datenbankdatei in Binärform ausgeliefert.

6.2 Report Übersicht

Die Übersicht der Reports und dessen Beschreibung wird laufend aktualisiert und weiterentwickelt.
Reports werden in der Darstellung

<Report-Type><Reportnummer>.<Version> gekennzeichnet.

Beispiel „V03.4“

Alle Reports haben ein einheitliches Layout mit:

- Kommentar auf der 1. Seite
- Überschrift auf jeder Seite
- Druckdatum
- Report Inhalt
- Fußteile mit Reportnummer (Spezifikation) und
- Seitenzahl

Die Reportspezifikation ist wichtig für die Kommunikation mit dem Support zur Problemanalyse.

Die jeweils aktuelle Übersicht wird mit der Softwareinstallation oder als Einzeldokument als PDF Dokument im Ordner Documents des Programm-Installationsverzeichnisses abgelegt.

Mit Aufruf des Moduls Viewer werden die anwendbaren Reports aus den, im Ordner Reports des Programm-Installationsverzeichnisses gespeicherten Vorlagen aktualisiert.

Folgende Report-Typen finden in asbLANtools Anwendung:

Report Type	Anwendung	Bemerkung
N	Netzwerk/Datenbank Reports	Netzwerk/Datenbankreports werden immer über den gesamten Inhalt einer DB ausgeführt. Alle anderen Report-Typen setzen die Selektion eines oder ggf. mehrerer Objekte (für einfache Reports) voraus.
V	Verzeichnisreports	
F	Datei Report	
S	Freigabe Report	
P	Printer Report	
L	Local Group Report	Lokale und universelle Gruppen vom Typ 2048
G	Global Group Report	Global und universelle Gruppen vom Typ 1024
A	Account Report	Maschinen- und Benutzer Accounts

Tabelle 6.8: Report Typen

6.3 Scan Filedaten

Jeder asb*LAN*tools Auftrag erzeugt mit jedem DatenScan ein Satz von Dateien, welche das jeweilige Scan-Ergebnis enthalten.

Es besteht die Möglichkeit in den Scanfiles mit einem Texteditor Änderungen vorzunehmen Die Daten der Scan File sollten ohne Kenntnis nicht verändert werden, da dadurch die DB Stabilität gefährdet ist.

Neu in der aktuellen Version ist, dass alle Inhaltsdaten eines Scans in einem File gespeichert werden.

```
     3 KB  NTFS-{T=20120313_161229}-{J=628d7a05eb3e499bb52dca7e79cc835e}-{IJob=8edfdcf28d604f1f85c724a3ad5a2853}.ILOG
40.881 KB  NTFS-{T=20120313_154253}-{J=628d7a05eb3e499bb52dca7e79cc835e}.LTX
14.107 KB  NTFS-{T=20120313_154253}-{J=628d7a05eb3e499bb52dca7e79cc835e}.SLOG
```

Wies aus diesem Auszug des Windows Explorers ersichtlich, werden alle Jobs mit einer Transaktionsnummer versehen. So erhält jeder Scanauftrag eine Scan-Transaktion, jeder anschließende Import-Job eine Import-Transaktionsnummer.

Filetypen:

- .LTX Scan Daten
- .SLOG Scan Logfile
- .ILOG Import Logfile
- .LTB Auftragsdatei (wird nur von asbLTS Service erstellt)

Bitte ändern Sie nicht die Namensstruktur des asbLANtools Datenfiles.- Dies führt zur Unbrauchbarkeit.

Die Namensstruktur asbLANtools besteht immer aus dem folgenden Schema:

<JobName>-{T=<Prozess-Zeit>}-{J=<Job-ID>}[-{IJob=Import-Job-ID}].<TypeName>

Die Dateien selbst können intern unterschiedliche Strukturen aufweisen.

Alles Datenfiles eines Jobs werden im Ordner „Data“(LTCmd & LTAdm) oder „Import“ (Scan Service) abgelegt.

Der Aufbau der Strukturen ist im technischen Handbuch beschrieben.

7 Fragen und Antworten

Lizenzierung

Wie komme ich zu einer Lizenz?

Lizenzen werden über die in asbLANtools verankerten LIC Files aktiviert.
Es können mehrere LIC Files für mehrere Domänen gleichzeitig verwendet werden.
Ein LIC File ist immer an

- Domänennamen oder
- SID der Domäne und
- Unternehmen

gebunden. Ein LIC File wird auf Basis der an asb Systemhaus gesandten Anforderungen erstellt. Dazu verwenden Sie die Schaltfläche „LIZENZ“ im Menü „Übersicht“.

Was wird lizenziert?

Alle asbLANtools Module unterliegen der Anwendung einer gültigen Lizenz. Die Programme zum Scan von Netzwerkdaten (Administrator, Scan Service, Batch Prozessor) werden von der internen Lizenzprüfung getestet.
Die Auswertemodule sind, eine gültige Lizenz vorausgesetzt, an beliebig vielen Arbeitsplätzen im Unternehmen anwendbar.

Leistungsanforderung

Die Anforderungen zur Arbeit mit den einzelnen Modulen sind sehr unterschiedlich. Grundsätzlich kann nur ein Richtwert gegeben werden. Detailaussagen sind nur im konkreten Fall, in Abhängigkeit vieler Parameter wie:

- Zustand, Lastverhalten und Geschwindigkeit des Netzwerkes;
- Leistungsfähigkeit der verwendeten Server;
- AD Replikation (Antwortzeiten);
- Eingesetzte Datenbank;
- Netzwerkantwortzeiten (sehr wichtig);
- Größe des Unternehmens und Datenverzeichnisse.

Nachfolgend ein Richtwert für asbLANtools Module (Aufgaben):

- Scan der Domäne : Minimal,
- Scan Filesystem : Stark abhängig von Netzwerkzustand, Netzwerklast durch asbLANtools selbst gering < 5%;
- Datenimport: Sehr leistungsfähiger MS SQL Import.
- Auswertung, Viewer: Mittlere Anforderungen (Datenansicht)
- Reports: Je nach aufgerufenen Report kann eine Auswertung Sekunden bis

Stunden dauern. Für den Umgang mit Reports sind Erfahrungen in der eigenen Umgebung zu sammeln.

- Zur Ermittlung des Leistungsbedarfes für einen Einsatz der Software im Unternehmen stellen wir eine Evaluierungsversion bereit.

Abbildungsverzeichnis

Abbildung 1.1: asbLANtools Objekt-Hierarchie 10
Abbildung 1.2: asbLANtools Administrator Überblick 15
Abbildung 1.3: Einführung asbLANtools Viewer 16
Abbildung 3.1: Setup Sprachauswahl 28
Abbildung 3.2: Setup Lizenzbedingungen 28
Abbildung 3.3: Datenbank anhängen 33
Abbildung 4.1: asbLANtools Startmenü Ikon 38
Abbildung 4.2: asbLANtools Startmenü 38
Abbildung 4.3: asbLANtools Lizenz anfordern 39
Abbildung 4.4: asbLANtools Lizenzdialog 40
Abbildung 4.5: asbLANtools Hauptmenü 41
Abbildung 4.6: Administrator Netzwerkansicht 42
Abbildung 4.7: Auftragsfenster im Administrator 43
Abbildung 4.8: Logfenster im Administrator 43
Abbildung 4.9: Datenbankauswahl 44
Abbildung 4.10: Zuweisen einer Datenquelle (MS SQL) 45
Abbildung 4.11: Zuweisen einer Offline-Datenquelle 45
Abbildung 4.12: asbLANtools Administrator 46
Abbildung 4.13: Administrator Menü Datenbank 47
Abbildung 4.14: Administrator Dialog Datenbank löschen 48
Abbildung 4.15: Administrator Dialog Statistik 48
Abbildung 4.16: Das Menü Auftrag 49
Abbildung 4.17: Das Menü Extras 49
Abbildung 4.18: Dialog, Verarbeitung 50
Abbildung 4.19: Dialog Protokoll 51
Abbildung 4.20: Dialog Datenquelle 52
Abbildung 4.21: Dialog Dateiübertragung 52
Abbildung 4.22: Dialog Lizenz 53
Abbildung 4.23: Dialog Versionen 53
Abbildung 4.24: Administrator Oberfläche 54
Abbildung 4.25: Administrator Scan Protokoll 57
Abbildung 4.26: Administrator Import Protokoll 58
Abbildung 4.27: asbLANtools Viewer Startbildschirm 60
Abbildung 4.28: Die asbLANtools Viewer Datenbankanmeldung 60
Abbildung 4.29: Der asbLANtools Viewer 61
Abbildung 4.30: Importierte Daten, Datum vom Scan u. Importprozess 63
Abbildung 4.31: Prüfregeln für importierte Daten 63
Abbildung 4.32: LTViewers: Auszug aus der Konfiguration 64
Abbildung 4.33: Bildaufbau unterbrechen 65
Abbildung 4.34: Die Suchfunktion des asbLANtools Viewer für Maschinen 66
Abbildung 4.37: Eigenschaftsfenster Zugriffsrechte für Dateien/ Verzeichnis 67
Abbildung 4.38: Eigenschaftsfenster Audit-Rechte für Dateien und Verzeichnisse 68
Abbildung 4.39: Die Benutzerkonten 69
Abbildung 4.40: Dialog Eigenschaften eines Benutzer 70
Abbildung 4.41: Dialog Benutzer ist Mitglied von Gruppe XY 70
Abbildung 4.42: Dialog Rechte für einen Benutzer 71
Abbildung 4.43: Dialog Ressourcen für einen Benutzer 71
Abbildung 4.44: Gruppendarstellung 72
Abbildung 4.45: Das Register Konto für eine globale Gruppe 72

Abbildung 4.46: Freigaben über lokale Gruppen *73*
Abbildung 4.47: Die Benutzerrechte und zugeordnete Gruppen *74*
Abbildung 4.48: Der asbLANtools Viewer, erfasste Dateisysteme *74*
Abbildung 4.49: LTViewer mit Verzeichnisberechtigungen *75*
Abbildung 4.50: Menü Dialog Treeview Ansicht *76*
Abbildung 4.51: Verzeichnisbaum Darstellung (Auszug) *77*
Abbildung 4.52: Berechtigungen eines Verzeichnisses *79*
Abbildung 4.53: asbLTViewer, Menüleiste mit ORC und TRC Option *79*
Abbildung 4.54: Beispiel einer Original-System ACL Liste *80*
Abbildung 4.55: Beispiel der konsolidierten Rechte Liste *80*
Abbildung 4.56: Querymanager *82*
Abbildung 4.57: Network Reports *83*
Abbildung 4.58: Auswahl eines selektiven Reports für ausgewählte Objekte *84*
Abbildung 4.59: Report-Layout Struktur *85*
Abbildung 4.60: Report Verarbeitung, Schematische Darstellung *86*
Abbildung 4.66: Reportaufruf , keine Daten *87*
Abbildung 4.67: asbLTCmd, integrierte Hilfe *89*
Abbildung 4.68: asbLTcmd Profile Steuerdaten *91*
Abbildung 4.69: Auszug aus einer Profile Steuerdatei für den LDAP Scan *93*
Abbildung 4.70: Auszug aus einer LDAP Dump Ausgabe *94*
Abbildung 4.71: Modul ScanService *95*
Abbildung 4.72: Modul Import Service *98*
Abbildung 5.1: Auswahl eines Domänencontrollers für den Scan Prozess *100*

Tabellenverzeichnis

Tabelle 4.1: asbLANtools Viewer Fensteraufteilung *46*
Tabelle 4.2: asbLANtools Viewer, Fensteraufteilung *62*
Tabelle 4.3: Suchfunktionen im LTViewer *66*
Tabelle 4.4: Ikonen: Baumstruktur- / Objektverhalten *76*
Tabelle 4.5: Ikonen und die Bedeutung für Verzeichnisauswertung *77*
Tabelle 4.6: asbLTViewer, List-Fenster und Inhalte für Filesysteme *78*
Tabelle 4.7: Reportansichten im LTViewer *85*
Tabelle 6.8: Report Typen *105*

Indexverzeichnis

A

Alt-Daten Übernahme 36
Analysefunktionen 69
Arbeitsweise 20
asbLAN*tools* Viewer 60
asbLANtools Funktionen 18
Auftragsdatei .LTB 97
Auswertung 36

B

Batch ausführen 55
Batch Befehl 54
Berücksichtigung im Design 16

D

Datenauswertung 37
Datenerfassung 37
Deinstallation 35
Demoversion 25
Drag und Drop 14

I

Informationen suchen 65
Installation 24, 27
Installationsvorbereitung 26

K

Konzept 20

L

Langzeitarchivierung 36
Leistungsumfang 20
Lizenzmodell 19, 24
Lizenzvertrag 5
Lizenzverwaltung 38

M

Migration 7
Modul Batch-Prozessor 88
Modul Importservice 97
Modul Reporting 82
Modul Viewer 58
Multidomänen 10

N

Neue DB anlegen 31

O

Objektklassen 10

R

Report Übersicht 104
Reports erstellen und drucken 82

S

Scanservice 55
Skriptgenerierung 67
Sprachauswahl 28
Standarddatenbank 44
Systemumgebung 18

U

Überprüfung einer DB 35
Update 35

V

Versionsstruktur 35
Visualisierung 37, 58
Voraussetzungen 24, 37

Z

Zugriffsberechtigungen 33